ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.В.04 Технология построения защищенных автоматизированных систем

Направление подготовки (специальность) **10.03.01 Информационная безопасность**

Профиль образовательной программы **Безопасность автоматизированных систем**

Форма обучения **очная**

СОДЕРЖАНИЕ

1. Конспект лекций……4

1.1 Лекция № 1 *Введение в предмет*……4

1.2 Лекция № 2 *Современные тенденции в программной инженерии*……6

1.3 Лекция № 3 *Нормативно методическое обеспечение создания АС*……11

1.4 Лекция № 4 *Стандарт жизненного цикла АС*……12

1.5 Лекция № 5 *Модели жизненного цикла АС*……13

1.6 Лекция № 6 *Оценка процессов создания АС*……17

1.7 Лекция № 7 *Общие принципы проектирования АС*……19

1.8 Лекция № 8 *Методология IDEF*……22

1.9 Лекция № 9 Методология eEPC……23

1.10 Лекция №10 *Постановка проблемы комплексного обеспечения информационной безопасности АС*……24

1.11 Лекция №11 *Особенности проектирования на современном уровне и синтез КСИБ*……27

1.12 Лекция №12 *Методы и методики проектирования КСИБ от НСД*……28

1.13 Лекция №13 *Методы и методики оценки КСИБ*……30

1.14 Лекция №14 *Аттестация АС по требованиям безопасности*……32

1.15 Лекция №15 *Особенности эксплуатации КСИБ на объекте защиты*……34

1.16 Лекция №16 *Модели защиты информации*……37

1.17 Лекция №17 *Реализация системы управления доступом*……38

2. Методические указания по проведению практических занятий ……43

2.1 Практическое занятие № ПЗ-1 *Введение в предмет* ……43

2.2 Практическое занятие № ПЗ-2-3 *Современные тенденции в программной инженерии* ……43

2.3 Практическое занятие № ПЗ-4 *Нормативно-методическое обеспечение создания АС*……43

2.4 Практическое занятие № ПЗ-5-6 *Стандарт жизненного цикла АС* ……44

2.5 Практическое занятие № ПЗ-7 *Модели жизненного цикла АС*……44

2.6 Практическое занятие № ПЗ-8-9 *Оценка процессов создания АС*……44

2.7 Практическое занятие № ПЗ-10 *Общие принципы проектирования АС*……45

2.8 Практическое занятие № ПЗ-11-12 *Методология IDEF* ……45

2.9 Практическое занятие № ПЗ-13 *Методология eEPC* ……45

2.10 Практическое занятие № ПЗ-14 *Постановка проблемы комплексного обеспечения информационной безопасности АС* ……..46

2.11 Практическое занятие № ПЗ-15 *Особенности проектирования на современном уровне и синтез КСИБ* …….....46

2.12 Практическое занятие № ПЗ-16-17 *Методы и методики проектирования КСИБ от НСД* …….....46

2.13 Практическое занятие № ПЗ-18 *Методы и методики оценки КСИБ* ……..46

2.14 Практическое занятие № ПЗ-19 *Особенности эксплуатации КСИБ на объекте защиты* ……..47

2.15 Практическое занятие № ПЗ-20-21 *Аттестация АС по требованиям безопасности*

……...……..47

2.16 Практическое занятие № ПЗ-22 *Модели защиты информации……47*

2.17 Практическое занятие № ПЗ-23 *Реализация системы управления доступом* …47

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция №1 (2 часа).

Тема: Введение в предмет.

1.1.1 Вопросы лекции:

1. Понятие автоматизированная система обработки информации и управления. Физический несанкционированный доступ. Логический несанкционированный доступ.. Принципы и законы управления

1.1.2 Краткое содержание вопросов:

В настоящее время информация, как результат автоматизированной обработки, с каждым годом определяет действия не только все большего числа людей, но и все большего числа технических систем, созданных человеком. Отсюда становится понятна актуальность задачи защиты информации в компьютерных системах с целью недопущения ее использования во вред людям и государству. Для эффективного решения данной задачи необходим тщательный анализ всех возможных способов несанкционированного доступа к информации в компьютерных системах, что позволяет своевременно принять меры для противодействия возможным угрозам. Здесь под несанкционированным доступом к информации понимается такой доступ, который нарушает правила использования информационных ресурсов компьютерной системы, установленные для ее пользователей.

Несанкционированный доступ является реализацией преднамеренной угрозы информационно- компьютерной безопасности и часто называется еще атакой или нападением на компьютерную систему.

Современные вычислительные системы являются территориально распределенными компьютерными сетями, объединяющими с помощью каналов связи различные компьютеры и локальные сети. Уязвимость распределенных вычислительных систем существенно превышает уязвимость автономных компьютеров. Это связано, прежде всего, с открытостью, масштабностью и неоднородностью самих компьютерных сетей. Соответственно существует немало способов атак на современные компьютерные сети. При этом количество угроз информационно- компьютерной безопасности и способов их реализации постоянно увеличивается.

Основными причинами здесь являются недостатки современных информационных технологий, а также неуклонный рост сложности программно-аппаратных средств. Приводимая ниже классификация не рассматривает атаки на информацию в полностью

открытых и не защищаемых компьютерных системах, так как способы их выполнения очевидны и не отличаются от обычных способов доступа к информационным ресурсам. Все возможные способы несанкционированного доступа к информации в защищаемых компьютерных системах можно классифицировать по следующим признакам:

1. По принципу несанкционированного доступа:

- физический несанкционированный доступ;
- логический несанкционированный доступ.

Физический несанкционированный доступ может быть реализован одним из следующих способов:

- преодоление рубежей территориальной защиты и доступ к незащищенным информационным ресурсам;
- хищение документов и носителей информации;
- визуальный перехват информации, выводимой на экраны мониторов и принтеры, а также подслушивание;
- перехват электромагнитных излучений.

Логический несанкционированный доступ предполагает логическое преодоление системы защиты ресурсов активной компьютерной сети. Основным предметом анализа в данном пособии будет являться логический несанкционированный доступ, как наиболее часто встречающийся в компьютерных и сетевых технологиях.

2. По положению источника несанкционированного доступа:

- несанкционированный доступ, источник которого расположен в локальной сети;
- несанкционированный доступ, источник которого расположен вне локальной сети.

В первом случае атака проводится непосредственно из любой точки локальной сети. Инициатором такой атаки чаще всего выступает санкционированный пользователь.

При подключении любой закрытой компьютерной сети к открытым сетям, например, к сети Интернет, высокую актуальность приобретают возможности несанкционированного вторжения в закрытую сеть из открытой. Подобный вид атак характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности или разных категорий. При ограничении доступа этих сетей друг к другу возникают угрозы нарушения установленных ограничений.

3. По режиму выполнения несанкционированного доступа:

- атаки, выполняемые при постоянном участии человека;

• атаки, выполняемые специально разработанными программами без непосредственного участия человека.

В первом случае для воздействия на компьютерную систему может использоваться и стандартное программное обеспечение. Во втором случае всегда применяются специально разработанные программы, в основу функционирования которых положена вирусная технология.

4. По типу используемых слабостей системы информационно- компьютерной безопасности:

• атаки, основанные на недостатках установленной политики безопасности;

• атаки, основанные на ошибках административного управления компьютерной сетью;

• атаки, основанные на недостатках алгоритмов защиты, реализованных в средствах информационно-компьютерной безопасности;

• атаки, основанные на ошибках реализации проекта системы защиты.

Недостатки политики безопасности означают, что разработанная для конкретной компьютерной сети политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий.

Под ошибками административного управления понимается некорректная организационная реализация или недостаточная административная поддержка принятой в компьютерной сети политики безопасности. Например, согласно политике безопасности должен быть запрещен доступ пользователей к определенному каталогу, а на самом деле по невнимательности администратора этот каталог доступен всем пользователям. Эффективные способы атак могут быть также основаны на недостатках алгоритмов защиты и ошибках реализации проекта системы информационно-компьютерной безопасности.

1. 1 Лекция №2 (2 часа).

Тема: Современные тенденции в программной инженерии.

1.1.1 Вопросы лекции:

1. Характеристики объекта внедрения. Технические характеристики проектов создания ПО. Организационные характеристики проектов создания ПО

1.1.2 Краткое содержание вопросов:

Накопленный к настоящему времени опыт создания систем ПО показывает, что это сложная и трудоемкая работа, требующая высокой квалификации участвующих в ней специалистов. Однако до настоящего времени создание таких систем нередко

выполняется на интуитивном уровне с применением неформализованных методов, основанных на искусстве, практическом опыте, экспертных оценках и дорогостоящих экспериментальных проверках качества функционирования ПО. По данным Института программной инженерии (Software Engineering Institute, SEI) в последние годы до 80% всего эксплуатируемого ПО разрабатывалось вообще без использования какой-либо дисциплины проектирования, методом "code and fix" (кодирования и исправления ошибок).

Проблемы создания ПО следуют из его свойств. Еще в 1975 г. Фредерик Брукс, проанализировав свой уникальный по тем временам опыт руководства крупнейшим проектом разработки операционной системы OS/360, определил перечень неотъемлемых свойств ПО: сложность, согласованность, изменяемость и незримость [1]. Что же касается современных крупномасштабных проектов ПО, то они характеризуются, как правило, следующими особенностями:

Характеристики объекта внедрения:

- структурная сложность (многоуровневая иерархическая структура организации) и территориальная распределенность;
- функциональная сложность (многоуровневая иерархия и большое количество функций, выполняемых организацией; сложные взаимосвязи между ними);
- информационная сложность (большое количество источников и потребителей информации (министерства и ведомства, местные органы власти, организации-партнеры), разнообразные формы и форматы представления информации, сложная информационная модель объекта - большое количество информационных сущностей и сложные взаимосвязи между ними), сложная технология прохождения документов;
- сложная динамика поведения, обусловленная высокой изменчивостью внешней среды (изменения в законодательных и нормативных актах, нестабильность экономики и политики) и внутренней среды (структурные реорганизации, текучесть кадров).

Технические характеристики проектов создания ПО:

- различная степень унифицированности проектных решений в рамках одного проекта;
- высокая техническая сложность, определяемая наличием совокупности тесно взаимодействующих компонентов (подсистем), имеющих свои локальные задачи и цели функционирования (транзакционных приложений, предъявляющих повышенные требования к надежности, безопасности и производительности, и приложений аналитической обработки (систем поддержки принятия решений), использующих нерегламентированные запросы к данным большого объема);

- отсутствие полных аналогов, ограничивающее возможность использования каких-либо типовых проектных решений и прикладных систем, высокая доля вновь разрабатываемого ПО;
- большое количество и высокая стоимость унаследованных приложений (существующего прикладного ПО), функционирующих в различной среде (персональные компьютеры, миникомпьютеры, мэйнфреймы), необходимость интеграции унаследованных и вновь разрабатываемых приложений;
- большое количество локальных объектов внедрения, территориально распределенная и неоднородная среда функционирования (СУБД, операционные системы, аппаратные платформы);
- большое количество внешних взаимодействующих систем различных организаций с различными форматами обмена информацией (налоговая служба, налоговая полиция, Госстандарт, Госкомстат, Министерство финансов, МВД, местная администрация).

Организационные характеристики проектов создания ПО:

- различные формы организации и управления проектом: централизованно управляемая разработка тиражируемого ПО, экспериментальные пилотные проекты, инициативные разработки, проекты с участием как собственных разработчиков, так и сторонних компаний на контрактной основе;
- большое количество участников проекта как со стороны заказчиков (с разнородными требованиями), так и со стороны разработчиков (более 100 человек), разобщенность и разнородность отдельных групп разработчиков по уровню квалификации, сложившимся традициям и опыту использования тех или иных инструментальных средств;
- значительная длительность жизненного цикла системы, в том числе значительная временная протяженность проекта, обусловленная масштабами организации-заказчика, различной степенью готовности отдельных ее подразделений к внедрению ПО и нестабильностью финансирования проекта;
- высокие требования со стороны заказчика к уровню технологической зрелости организаций-разработчиков (наличие сертификации в соответствии с международными и отечественными стандартами).

В конце 60-х годов прошлого века в США было отмечено явление под названием "software crisis" (кризис ПО). Это выражалось в том, что большие проекты стали выполняться с отставанием от графика или с превышением сметы расходов, разработанный продукт не обладал требуемыми функциональными возможностями, производительность его была низка, качество получаемого программного обеспечения не устраивало потребителей.

Аналитические исследования и обзоры, выполняемые в течение ряда последних лет ведущими зарубежными аналитиками, показывали не слишком обнадеживающие результаты. Так, например, результаты исследований, выполненных в 1995 году компанией Standish Group, которая проанализировала работу 364 американских

корпораций и итоги выполнения более 23 тысяч проектов, связанных с разработкой ПО, выглядели следующим образом:

- только 16,2% завершились в срок, не превысили запланированный бюджет и реализовали все требуемые функции и возможности;
- 52,7% проектов завершились с опозданием, расходы превысили запланированный бюджет, требуемые функции не были реализованы в полном объеме;
- 31,1% проектов были аннулированы до завершения;
- для двух последних категорий проектов бюджет среднего проекта оказался превышенным на 89%, а срок выполнения - на 122%.

В 1998 году процентное соотношение трех перечисленных категорий проектов лишь немного изменилось в лучшую сторону (26%, 46% и 28% соответственно).

В последние годы процентное соотношение трех перечисленных категорий проектов также незначительно изменяется в лучшую сторону, однако, по оценкам ведущих аналитиков, это происходит в основном за счет снижения масштаба выполняемых проектов, а не за счет повышения управляемости и качества проектирования.

В числе причин возможных неудач, по мнению разработчиков, фигурируют:

- нечеткая и неполная формулировка требований к ПО;
- недостаточное вовлечение пользователей в работу над проектом;
- отсутствие необходимых ресурсов;
- неудовлетворительное планирование и отсутствие грамотного управления проектом;
- частое изменение требований и спецификаций;
- новизна и несовершенство используемой технологии;
- недостаточная поддержка со стороны высшего руководства;
- недостаточно высокая квалификация разработчиков, отсутствие необходимого опыта.

Объективная потребность контролировать процесс разработки сложных систем ПО, прогнозировать и гарантировать стоимость разработки, сроки и качество результатов привела в конце 60-х годов прошлого века к необходимости перехода от кустарных к индустриальным способам создания ПО и появлению совокупности инженерных методов и средств создания ПО, объединенных общим названием "программная инженерия" (software engineering). В основе программной инженерии лежит одна фундаментальная идея: проектирование ПО является формальным процессом, который можно изучать и совершенствовать. Освоение и правильное применение методов и средств создания ПО позволяет повысить его качество, обеспечить управляемость процесса проектирования ПО и увеличить срок его жизни.

В то же время, попытки чрезмерной формализации процесса, а также прямого заимствования идей и методов из других областей инженерной деятельности (строительства, производства) привели к ряду серьезных проблем. После двух десятилетий напрасных ожиданий повышения продуктивности процессов создания ПО, возлагаемых на новые методы и технологии, специалисты в индустрии ПО пришли к пониманию, что фундаментальная проблема в этой области - неспособность эффективного управления проектами создания ПО. Невозможно достичь удовлетворительных результатов от применения даже самых совершенных технологий и инструментальных средств, если они применяются бессистемно, разработчики не обладают необходимой квалификацией для работы с ними, и сам проект выполняется и управляется хаотически, в режиме "тушения пожара". Бессистемное применение технологий создания ПО (ТС ПО), в свою очередь, порождает разочарование в используемых методах и средствах (анализ мнений разработчиков показывает, что среди факторов, влияющих на эффективность создания ПО, используемым методам и средствам придается гораздо меньшее значение, чем квалификации и опыту разработчиков). Если в таких условиях отдельные проекты завершаются успешно, то этот успех достигается за счет героических усилий фанатично настроенного коллектива разработчиков. Постоянное повышение качества создаваемого ПО и снижение его стоимости может быть обеспечено только при условии достижения организацией необходимой технологической зрелости, создании эффективной инфраструктуры как в сфере разработки ПО, так и в управлении проектами. В соответствии с моделью SEI CMM (Capability Maturity Model), в хорошо подготовленной (зрелой) организации персонал обладает технологией и инструментарием оценки качества процессов создания ПО на протяжении всего жизненного цикла ПО и на уровне всей организации.

Одна из причин распространенности "хаотического" процесса создания ПО - стремление сэкономить на стадии разработки, не затрачивая времени и средств на обучение разработчиков и внедрение технологического процесса создания ПО. Эти затраты до недавнего времени были довольно значительными и составляли, по различным оценкам (в частности, Gartner Group), более $100 тыс. и около трех лет на внедрение развитой ТС ПО, охватывающей большинство процессов жизненного цикла ПО, в многочисленной команде разработчиков (до 100 чел.). Причина - в "тяжести" технологических процессов. "Тяжелый" процесс обладает следующими особенностями:

- необходимость документировать каждое действие разработчиков;
- множество рабочих продуктов (в первую очередь - документов), создаваемых в бюрократической атмосфере;
- отсутствие гибкости;
- детерминированность (долгосрочное детальное планирование и предсказуемость всех видов деятельности, а также распределение человеческих ресурсов на длительный срок, охватывающий большую часть проекта.

Альтернативой "тяжелому" процессу является адаптивный (гибкий) процесс, основанный на принципах "быстрой разработки ПО", интенсивно развиваемых в последнее десятилетие.

1. 1 Лекция №3 (2 часа).

Тема: Нормативно-методическое обеспечение создания АС

1.1.1

Вопросы лекции: Нормативно-методическое обеспечение АС. Международные стандарты. Стандарты Российской Федерации. Стандарты организации-заказчика

1.1.2 Краткое содержание вопросов:

Разработка больших проектов, связанная с работой коллективов размером в несколько десятков и даже сотен человек из нескольких организаций, возможна при наличие совокупности нормативно-методических документов, регламентирующих различные аспекты процессов деятельности разработчиков. Комплекс таких документов называют *нормативно-методическим обеспечением (НМО).*Эти документы регламентируют:

порядок разработки, внедрения и сопровождения АС;

общие требования к составу АС и связям между ее компонентами, а также к его качеству;

виды, состав и содержание проектной и рабочей документации.

Все входящие в состав НМО документы классифицируются по следующим признакам:

виду регламентации (стандарт, руководящий документ, положение, инструкция и т.п.);

статусу регламентирующего документа (международный, отраслевой, предприятия);

области действия документа (заказчик, подрядчик, проект);

• объекту регламентации или методического обеспечения.

Нормативной базой НМО являются:

международные стандарты ISO/IEC (ISO — International Organization of Standardization — Международная организация по стандартизации, IEC — International Electrotechnical Commission — Международная комиссия по электротехнике);

стандарты Российской Федерации ГОСТ Р;

стандарты организации-заказчика.

В СССР в 70-е годы прошлого века процесс создания ПО регламентировался стандартами ГОСТ ЕСПД (Единой Системы Программной Документации — серия ГОСТ 19.XXX), которые были ориентированы на класс относительно простых программ небольшого объема, создаваемых отдельными программистами. В настоящее время эти стандарты устарели концептуально и по форме, их сроки действия закончились и использование нецелесообразно.

Процессы создания АС регламентированы стандартами **ГОСТ 34.601-90** «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»; **ГОСТ 34.602-89** «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» и **ГОСТ 34.603—92**«Информационная технология. Виды испытаний автоматизированных систем».

Однако процессы создания ПО для современных распределенных систем, функционирующих в неоднородной среде, в этих стандартах отражены недостаточно, а отдельные их положения явно устарели. В результате для каждого серьезного проекта приходится создавать комплекты нормативных и методических документов, регламентирующих процессы, этапы, работы и документы конкретных программных продуктов, поэтому в отечественных разработках целесообразно использовать современные международные стандарты.

1. 1 Лекция №4 (2 часа).

Тема: Стандарт жизненного цикла АС.

1.1.1 Вопросы лекции: *Жизненный цикл информационной системы. Документирование. Управление конфигурацией. обеспечение качества*

1.1.2 Краткое содержание вопросов:

Понятие жизненного цикла (ЖЦ) является одним из ключевых понятий методологии проектирования информационных систем. ***Жизненный цикл информационной системы*** – это непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации .

Основным стандартом, определяющим структуру жизненного цикла, является ГОСТ Р ИСО/МЭК 12207-02. Согласно стандарту структура жизненного цикла основывается на трех группах процессов:

· ***основные процессы*** (заказ, поставка, разработка, эксплуатация, сопровождение);

· ***вспомогательные процессы*** (обеспечивают выполнение основных процессов):

о *документирование* – работы по разработке, выпуску, редактированию, распространению и сопровождению документов, в которых нуждаются все заинтересованные лица;

о *управление конфигурацией* (конфигурационное управление) включает работы: определение и установление состояния программных объектов в системе; управление изменениями и выпуском объектов; обеспечение полноты, совместимости и правильности объектов; управление хранением, обращением и поставкой объектов;

о *обеспечение качества* – работы по обеспечению соответствия создаваемой системы и реализуемых процессов жизненного цикла установленным требованиям и утвержденным планам;

о *верификация* – работы соответствующего субъекта (заказчика, поставщика или независимой стороны) по проверке соответствия создаваемых промежуточных результатов установленным требованиям по мере реализации проекта. Различают верификацию договора, процесса, требований, проекта, системы, сборки системы и документации;

о *аттестация* – работы соответствующего субъекта по проверке полного соответствия требований и конечного продукта функциональному назначению системы;

o *совместный анализ* – работы по оценке состояния или результатов какой-либо работы (системы);

o *аудит* – работы независимых (по отношению к проекту) экспертов по определению соответствия деятельности субъекта принятым требованиям, планам и условиям договора;

o *разрешение проблем* – работы по анализу и устранению проблем, обнаруженных при реализации проекта;

· ***организационные*:**

o *управление проектами* – работы по планированию и управлению процессами, включая контроль, проверку и оценку выполненных работ с формированием отчетности;

o *создание инфраструктуры проекта* – работы по установлению и обеспечению инфраструктуры, необходимой для любого другого процесса. Инфраструктура может содержать технические и программные средства, инструментальные средства, методики, стандарты и условия для разработки, эксплуатации или сопровождения системы;

o *усовершенствование* – работы по оценке, контролю и улучшению процессов жизненного цикла;

o *обучение* – работы по планированию и проведению обучения персонала, включая разработку учебных материалов. При этом под персоналом понимаются не только конечные пользователи, которые будут эксплуатировать систему, но и разработчики системы. Например, разработчики должны быть обучены технологиям и средствам программирования, принятым в организации, и даже обучены правильно внедрять и обучать конечных пользователей работе с системой. Как бы это ни парадоксально звучало, но обучать правильной методике и приемам обучения тоже необходимо.

1. 1 Лекция №5 (2 часа).

Тема: Модели жизненного цикла АС.

1.1.1 Вопросы лекции: Модель ЖЦ АС. Каскадные модели ЖЦ АС.

Итерационные модели ЖЦ АС. Эволюционная модель ЖЦ АС.

1.1.2 Краткое содержание вопросов:

К настоящему времени наибольшее распространение получили следующие модели (стратегии) жизненного цикла

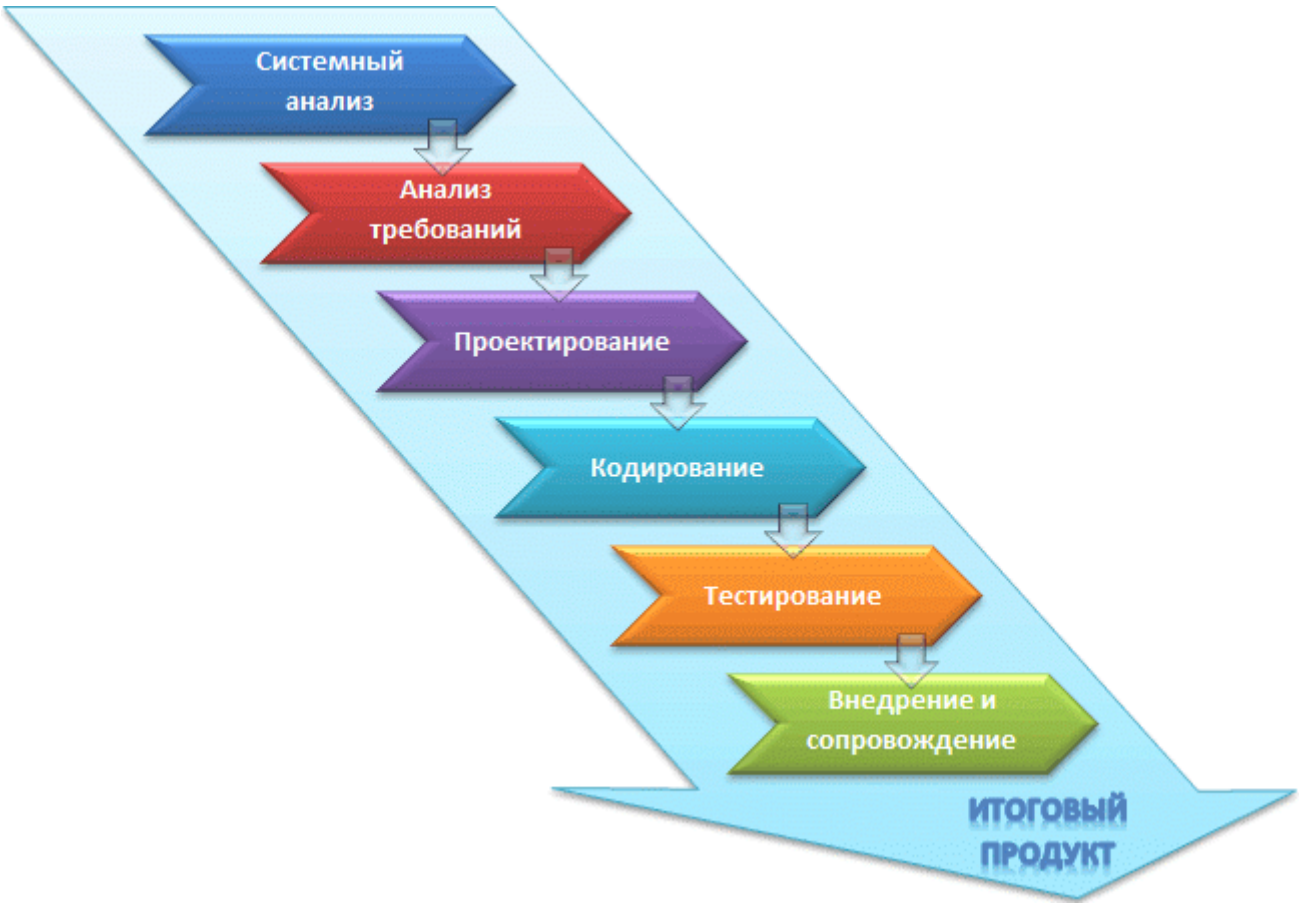
- каскадная;

- инкрементная;

- спиральная.

Дальнейшее рассмотрение моделей жизненного цикла ведется с использованием терминологии классического жизненного цикла

Аскадная стратегия (однократный проход, водопадная или классическая модель) подразумевает линейную последовательность выполнения стадий создания информационной системы (рис.3.1). Другими словами, переход с одной стадии на следующую происходит только после того, как будет полностью завершена работа на текущей.



Каскадная стратегия

Данная модель применяется при разработке информационных систем, для которых в самом начале разработки можно достаточно точно и полно сформулировать все требования.

Достоинства модели:

- на каждой стадии формируется законченный набор документации, программного и аппаратного обеспечения, отвечающий критериям полноты и согласованности;

- выполняемые в четкой последовательности стадии позволяют уверенно планировать сроки выполнения работ и соответствующие ресурсы (денежные, материальные и людские).

Недостатки модели:

- реальный процесс разработки информационной системы редко полностью укладывается в такую жесткую схему. Особенно это относится к разработке нетиповых и новаторских систем;

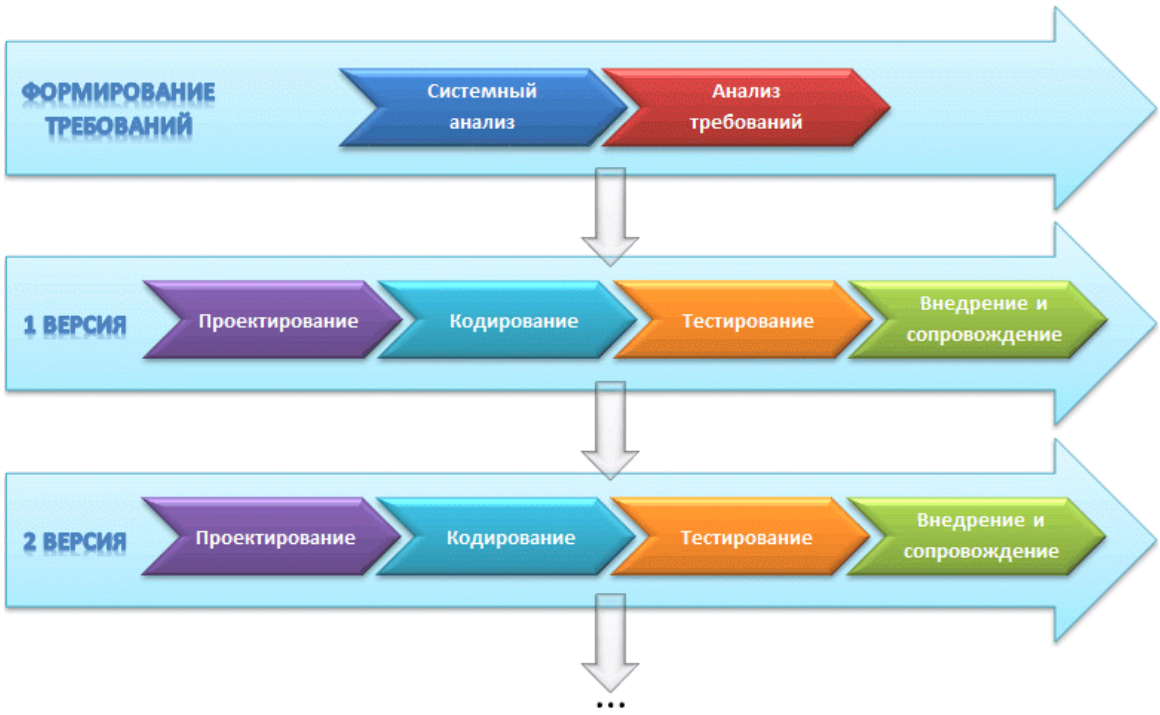
- жизненный цикл основан на точной формулировке исходных требований к информационной системе. Реально в начале проекта требования заказчика определены лишь частично;

- основной недостаток – результаты разработки доступны заказчику только в конце проекта. В случае неточного изложения требований или их изменения в

течение длительного периода создания ИС заказчик получает систему, не удовлетворяющую его потребностям.

Инкрементная стратегия

Инкрементная стратегия (англ. increment – увеличение, приращение) подразумевает разработку информационной системы с линейной последовательностью стадий, но в несколько инкрементов (версий), т. е. с запланированным улучшением продукта.



Инкрементная стратегия

В начале работы над проектом определяются все основные требования к системе, после чего выполняется ее разработка в виде последовательности версий. При этом каждая версия является законченным и работоспособным продуктом. Первая версия реализует часть запланированных возможностей, следующая версия реализует дополнительные возможности и т. д., пока не будет получена полная система.

Данная модель жизненного цикла характерна при разработке сложных и комплексных систем, для которых имеется четкое видение (как со стороны заказчика, так и со стороны разработчика) того, что собой должен представлять конечный результат (информационная система). Разработка версиями ведется в силу разного рода причин:

- отсутствия у заказчика возможности сразу профинансировать весь дорогостоящий проект;

- отсутствия у разработчика необходимых ресурсов для реализации сложного проекта в сжатые сроки;

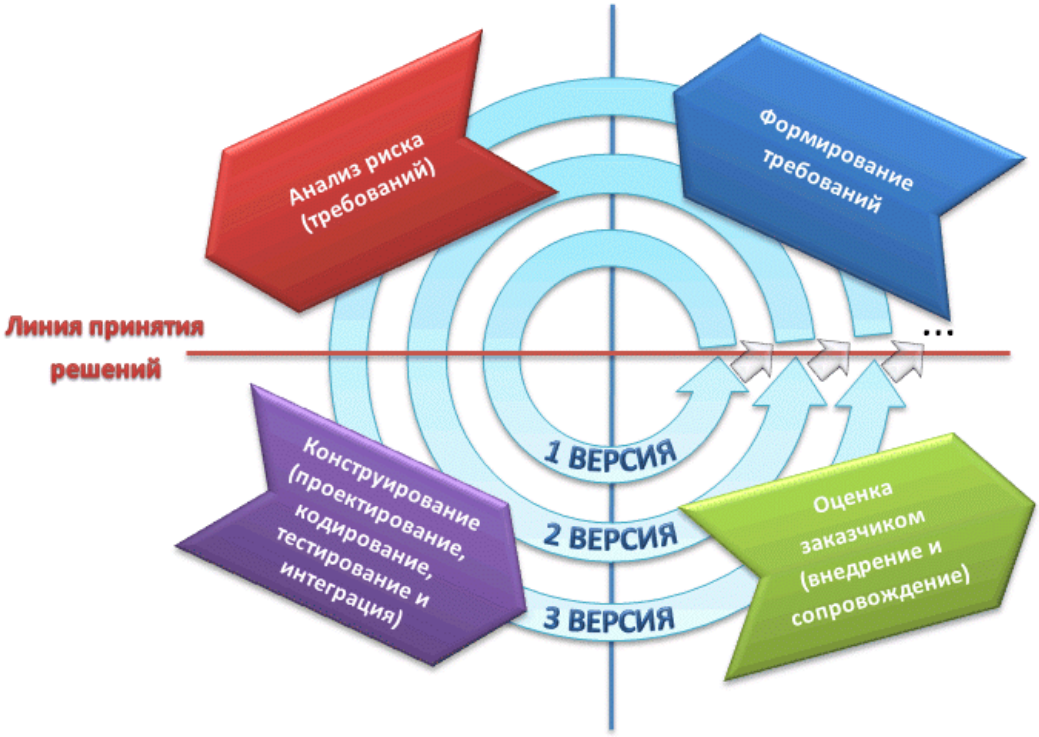
- требований поэтапного внедрения и освоения продукта конечными пользователями. Внедрение всей системы сразу может вызвать у ее пользователей

неприятие и только «затормозить» процесс перехода на новые технологии. Образно говоря, они могут просто «не переварить большой кусок, поэтому его надо измельчить и давать по частям».

Достоинства и ***недостатки*** этой стратегии такие же, как и у классической. Но в отличие от классической стратегии заказчик может раньше увидеть результаты. Уже по результатам разработки и внедрения первой версии он может незначительно изменить требования к разработке, отказаться от нее или предложить разработку более совершенного продукта с заключением нового договора.

Спиральная стратегия

Спиральная стратегия (эволюционная или итерационная модель, автор Барри Боэм, 1988 г.) подразумевает разработку в виде последовательности версий, но в начале проекта определены не все требования. Требования уточняются в результате разработки версий.



Спиральная стратегия

Данная модель жизненного цикла характерна при разработке новаторских (нетиповых) систем. В начале работы над проектом у заказчика и разработчика нет четкого видения итогового продукта (требования не могут быть четко определены) или стопроцентной уверенности в успешной реализации проекта (риски очень велики). В связи с этим принимается решение разработки системы по частям с возможностью изменения требований или отказа от ее дальнейшего развития. Как видно из рис.3.3, развитие проекта может быть завершено не только после стадии внедрения, но и после стадии анализа риска.

Достоинства модели:

- позволяет быстрее показать пользователям системы работоспособный продукт, тем самым, активизируя процесс уточнения и дополнения требований;

- допускает изменение требований при разработке информационной системы, что характерно для большинства разработок, в том числе и типовых;

- обеспечивает большую гибкость в управлении проектом;

- позволяет получить более надежную и устойчивую систему. По мере развития системы ошибки и слабые места обнаруживаются и исправляются на каждой итерации;

- позволяет совершенствовать процесс разработки – анализ, проводимый в каждой итерации, позволяет проводить оценку того, что должно быть изменено в организации разработки, и улучшить ее на следующей итерации;

- уменьшаются риски заказчика. Заказчик может с минимальными для себя финансовыми потерями завершить развитие неперспективного проекта.

Недостатки модели:

- увеличивается неопределенность у разработчика в перспективах развития проекта. Этот недостаток вытекает из предыдущего достоинства модели;

- затруднены операции временного и ресурсного планирования всего проекта в целом. Для решения этой проблемы необходимо ввести временные ограничения на каждую из стадий жизненного цикла. Переход осуществляется в соответствии с планом, даже если не вся запланированная работа выполнена. План составляется на основе статистических данных, полученных в предыдущих проектах и личного опыта разработчиков.

1. 1 Лекция №6 (2 часа).

Тема: Оценка процессов создания АС.

1.1.1 Вопросы лекции: Понятие зрелости процессов создания АС. Модель оценок зрелости.

1.1.2 Краткое содержание вопросов:

Зрелость процесса – степень их управляемости, контролируемости и эффективности.

Модель технологической зрелости организации CMM (capability maturity model), определив в ней 5 уровней зрелости организации и их отличительные черты. Оценка технологической зрелости может использоваться:

заказчиком при отборе лучших исполнителей;

компаниями — производителями АС для систематической оценки состояния своих технологических процессов;

компаниями, решившими пройти аттестацию;

аудиторами для определения стандартной процедуры аттестации и проведения необходимых оценок.

1.2. Модель оценки зрелости CMM.

CMM – описательная модель, которая описывает ключевые атрибуты и определяет на каком уровне технологической зрелости находится организация.

постоянное
совершенствование
прогнозирование
результатов
стандартизация
процессов
упорядочение
процессов

На первом уровне основные процессы создания и сопровождения АС носят случайный характер и выполняются хаотично. Успех выполнения проекта всецело зависит от индивидуальных усилий персонала. В организации, как правило, не существует стабильной среды необходимой для создания и сопровождения АС. Успех проекта зависит от степени энергичности и опыта руководства, и профессионального уровня

исполнителей.

На втором уровне процессы управления проектом позволяют обеспечивать текущий контроль стоимости проекта графика его выполнения и выполняемых функций. Планирование проектных работ и управление новыми проектами базируется на опыте успешно выполненных аналогичных проектов. Основной особенностью второго уровня является наличие формализованных и документированных эффективных процессов управления проектами. Эффективными могут называться процессы, которые документированы, реально используются, поддаются количественной оценке и пригодные для модернизации. Необходимо, чтобы персонал был обучен к их применению. Группы процессов второго уровня:

управление требованиями,
управление конфигурацией,
планирование проекта,
мониторинг и контроль проекта,
управление контрактами,
изменение и анализ,
обеспечение качества процесса и продуктов.

На третьем уровне процессы создания АС документированы, стандартизованы и представляют собой единую технологическую систему обязательную для всех подразделений организации во всех проектах используется опробованная, утвержденная и возведенная в статус стандарта единая технология создания и сопровождения АС. Группы процессов третьего уровня: +2 уровня,

спецификация требований,
интеграция продукта,
верификация,
аттестация,
стандартизация процессов организации,

обучение,

интегрированное управление проектом,

управление рисками,

анализ и принятие решений.

На этом уровне в организации создается специальная группа, ответственная за состав операций из которых состоят процессы – группа по разработке процессов создания АС.

На четвертом уровне управление должно обеспечивать выполнение процессов в рамках заданного качества. Группы процессов четвертого уровня: +3 уровня,

управление производительностью и продуктивностью,

количественное управление проектом.

В рамках всей организации разрабатывается единая программа количественного контроля производительности создания АС и ее качества. Для облегчения анализа процессов создается единая база данных процессов создания и сопровождения АС для всех проектов, выполняемых в организации. Разрабатываются универсальные методики количественной оценки производительности процессов и качества их выполнения. Это позволяет проводить количественный анализ и оценку процессов создания и сопровождения АС.

На пятом уровне проводится последовательное усовершенствование и модернизация процессов создания и сопровождения ПО и АС. В целях плановой модернизации технологии создания АС в организации создается специальное подразделение основными обязанностями которого является сбор данных по выполнению процессов, их анализ, модернизация имеющихся и создание новых процессов, их проверка на пилотных проектах и придание им статуса стандартов предприятия. Группы процессов: +4 уровня,

внедрение технологических и организационных инноваций,

причинно-следственный анализ и разрешение проблем.

1. 1 Лекция №7 (2 часа).

Тема: Общие принципы проектирования АС.

1.1.1 Вопросы лекции: Структурный подход к анализу и проектированию АС. Визуальное моделирование.Языки моделирования.

1.1.2 Краткое содержание вопросов:

Основной проблемой, которую приходится решать при создании больших систем любой природы является проблема сложности. Правильная декомпозиция системы является главным способом преодоления сложностей больших систем.

Понятие правильно по отношению к декомпозиции означает следующее:

Количество связей между отдельными подсистемами должно быть минимальным

Связанность отдельных частей внутри каждой подсистемы должно быть максимальным.

Структура системы должна быть такой, чтобы все взаимодействия между ее подсистемами укладывались в ограничения:

Каждая подсистема должна инкапсулировать своё содержимое

Каждая подсистема должна иметь четко определенный интерфейс с другими подсистемами

Существует 2-а основных подхода к декомпозиции систем:

Функционально-модульный (структурный подход) – в основу положен принцип функциональной декомпозиции при которой структура системы описывает в терминах иерархии ее функций и передачей информацией между отдельными функциональными элементами

Объектно-ориентированный подход – использует объектную декомпозицию, при которой структура системы описывается в терминах объекта и связей между ними, а поведение системы описывается в терминах обмена сообщениями между объектами.

1.2. Визуальное моделирование.

Моделирование – процесс создания формализованного описания системы в виде совокупности моделей.

Модель должна давать полное, точное и адекватное описание системы, имеющая конкретное назначение.

Формальное определение модели:

«M» — есть модель системы «S», если «M» может быть использована для получения ответов на вопросы относительно «S» с точностью «A».

Визуальное моделирование – это способ восприятия проблем с помощью зримых абстракций, воспроизводящих понятия и объекты реального времени.

Визуальные модели — это средства для визуализации, описания, проектирования и документирование архитектуры системы.

Архитектура системы – это набор основных правил, определяющих организацию системы:

совокупность структурных элементов системы и связи между ними;

поведение элементов системы в процессе их взаимодействия;

иерархия подсистем, объединяющих структурные элементы;

архитектурный стиль (используемые методы и средства описания архитектуры);

Язык моделирования – это:

Элементы модели – функциональные концепции моделирования и их семантику

Нотация (система обозначений) – визуальное представление элементов моделирования

Руководство по использованию правило применение элементов в рамках построения тех или иных типов моделей

Моделирование – процесс создания формализованного описания системы в виде совокупности моделей.

Модель должна давать полное, точное и адекватное описание системы, имеющая конкретное назначение. Это назначение вытекает из формального определения модели.

«M» — есть модель системы «S», если «M» может быть использована для получения ответов на вопросы относительно «S» с точностью «A».

Визуальное моделирование – это способ восприятия проблем с помощью зримых абстракций, воспроизводящих понятия и объекты реального времени.

Визуальные модели — это средства для визуализации, описания, проектирования и документирование архитектуры системы.

Архитектура системы – это набор основных правил, определяющих организацию системы:

Совокупность структурных элементов системы и связи между ними

Поведение элементов системы в процессе их взаимодействия

Иерархия подсистем, объединяющих структурные элементы

Архитектурный стиль (используемые методы и средства описания архитектуры)

Язык моделирования – это:

Элементы модели – функциональные концепции моделирования и их симантику

Нотация (система обозначений) – визуальное представление элементов моделирования

Руководство по использованию правило применение элементов в рамках построения тех или иных типов моделей

В процессе создания АС организации используют следующие виды моделей: модели ***«AS-IS» (как есть)*** – отражает на данный момент процесс, ***«AS-TO-BE»*** — отражает представление о новых процессах и технологиях работы организации. Переход от модели «AS-IS» до «AS-TO-BE» может выполняться двумя способами:

Совершенствованием существующих технологий на основе оценки их эффективности;

Радикальном изменении технологий и перепроектирования бизнеПЗ-процесса.

1. 1 Лекция №8 (1 часа).

Тема: Методология IDEF.

1.1.1 Вопросы лекции:

Структурный синтез систем. Методологии структурного синтеза. IDEF0. IDEF1. IDEF1x. DEF2.IDEF3.IDEF4.IDEF5.

1.1.2 Краткое содержание вопросов:

Взаимная совокупность методик и моделей концептуального проектирования IDEF разработана в США по программе Integrated Computer-Aided Manufacturing. В настоящее время имеются методики функционального, информационного и поведенческого моделирования и проектирования, в которые входят следующие IDEF-модели:

IDEFO - Функциональное моделирование (Function Modeling Method). Наиболее известной реализацией IDEF0 является методология SADT (Structured Analysis and Design Technique). Эта методика рекомендуется для начальных стадий проектирования сложных искусственных систем управления, производства, бизнеса, включающих людей, оборудование, программное обеспечение.

IDEF1 и IDEF1X - Информационное моделирование (Information and Data Modeling Method). В IDEF1X имеется ясный графический язык для описания объектов и отношений в приложениях, так называемый язык диаграмм "сущность-связь".

IDEF2 - Поведенческое моделирование (Simulation Modeling Method). В основе поведенческого моделирования лежат модели и методы имитационного моделирования систем массового обслуживания, сети Петри.

IDEF3 - Моделирование деятельности (Process Flow and Object Stale Description Capture Method). В методике детализируется ответ на вопрос не "что система делает", а "как система это делает".

IDEF4 - Объективно-ориентированное проектирование (Object-oriented Design Method). Модель предоставляет пользователю графический язык для изображения классов, диаграмм наследования, таксономии методов.

IDEF5 - Систематизация объектов приложения (Ontology Description Capture Method). Модель представляет онтологической информации приложения в удобном для пользователя виде, Для этого используются символические обозначения (дескрипторы) объектов, их ассоциаций, ситуаций и схемный язык описания отношений классификации, "часть-целое", перехода и т. п. В методике имеются правила связывания объектов (термов) в предложения и аксиомы интерпретации термов.

IDEF6 - Использование рационального опыта проектирования (Design Rational Capture Method). Способствует предотвращению структурных ошибок.
IDEF8 - Взаимодействие человека и системы (Human-System Interaction Design). Модель предназначена для проектирования диалогов человека и технической системы.
IDEF9 - Учет условий и ограничений (Business Constraint Discovery). Модель предназначена для анализа имеющихся условий и ограничений (в том числе физических, юридических, политических) и их влияния на принимаемые решения в процессе реинжиниринга.
IDEF14 - Моделирование вычислительных сетей (Network Design). Модель предназначена для представления и анализа данных при проектировании вычислительных сетей на графическом языке с описанием конфигураций, очередей, сетевых компонентов, требований к надежности и т.п.

1. 1 Лекция №9 (2 часа).

Тема: Методология eEPC.

1.1.1 Вопросы лекции:

Особенности методологии eEPC. Нотация методологии eEPC.

1.1.2 Краткое содержание вопросов:

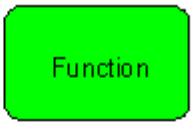
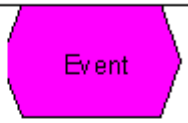
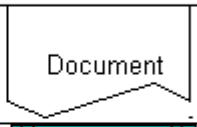
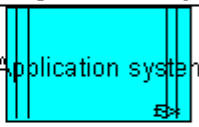
В настоящее время существует множество различных принципов графического представления бизнеПЗ-процессов, именуемых нотациями. Почему их много? Этот вопрос уже десятки лет задает себе каждый, кто сталкивается с необходимостью описать бизнеПЗ-процессы. Давайте разберемся с причинами. Их три (на мой взгляд):

Разные задачи. Не все нотации одинаково удобны для решения различных задач. Например, нотация может быть удобна для бизнеПЗ-процесса верхнего уровня и совсем не удобной для описания рабочего процесса.

Разные разработчики таких нотаций. В разное время разные разработчики пытались придумать новые принципы описания схем. Делали они это из благих побуждений, когда на практике сталкивались с ситуацией, когда используемая ими нотация не может отразить необходимых тонкостей (либо не наглядно). Иногда в процессе эволюции такие нотации стали как бы параллельными, т.е. выглядят по разному, а задачи решают одинаковые.

Стремление выделиться. Это когда по непонятным причинам вдруг появляется новая нотация, не имеющая в себе ничего выдающегося, но, почему-то продвигающаяся ее создателем как совершеннейшее ноу-хау. Такое происходит до сих пор.

Нотация ARIS eEPC (extended Event Driven Process Chain) – расширенная нотация описания цепочки процесса, управляемого событиями. Нотация разработана специалистами компании IDS Scheer AG (Германия), в частности профессором Шеером.

№	Наименование	Описание	Графическое представление
1	Функция	Объект «Функция» служит для описания функций (процедур, работ), выполняемых подразделениями/сотрудниками предприятия.	
2	Событие	Объект «Событие» служит для описания реальных состояний системы, влияющих и управляющих выполнением функций	
3	Организационная единица	Объект, отражающий различные организационные звенья предприятия (например, управление или отдел)	
4	Документ	Объект, отражающий реальные носители информации, например бумажный документ	
5	Прикладная система	Объект отражает реальную прикладную систему, используемую в рамках технологии выполнения функции	
6	Кластер информации	Объект характеризует данные, как набор сущностей и связей между ними. Используется для создания моделей данных	
7	Стрелка связи между объектами	Объект описывает тип отношений между другими объектами, например – активацию выполнения функции некоторым событием	
8	Логическое «И»	Логический оператор, определяющий связи между событиями и функциями в рамках процесса. Позволяет описать ветвление процесса	
9	Логическое «ИЛИ»	Логический оператор, определяющий связи между событиями и функциями в рамках процесса. Позволяет описать ветвление процесса	
10	Логическое исключающее «ИЛИ»	Логический оператор, определяющий связи между событиями и функциями в рамках процесса. Позволяет описать ветвление процесса	

1. 1 Лекция №10 (2 часа).

Тема: Постановка проблемы комплексного обеспечения информационной безопасности АС.

1.1.1 Вопросы лекции:

Понятия «комплексности» и «системности». Основополагающие меры комплексной безопасности АС.

1.1.2 Краткое содержание вопросов:

Непрерывность защиты

Защита информации — не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а *непрерывный целенаправленный процесс,* предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных “закладок” и других средств преодоления системы защиты после восстановления ее функционирования.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Разделение функций

Принцип Разделения функций, требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущения сговора и разграничению ответственности между этими сотрудниками.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их

разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты

не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

1. 1 Лекция №11 (2 часа).

Тема: Особенности проектирования на современном уровне и синтез КСИБ.

1.1.1 Вопросы лекции:

Основные подходы при проектировании. Общая характеристика проблемы синтеза систем защиты. Типовая структура КСЗИ от несанкционированного доступа.

1.1.2 Краткое содержание вопросов:

Выделяют следующие подходы к проектированию:

1. Использование типовых СЗИ.

Выбирается один из имеющихся типовых проектов полной СЗИ. Осуществляется привязка типового проекта к условиям конкретной АС.

Целесообразно применять, когда: Требования к ЗИ не очень высокие. Строго определенная структура АС. Архитектура АС близка к одной из типовых. Требования и условия защиты во всех однотипных ТСК однородны.

2. Использование типовых структурно-ориентированных компонентов СЗИ.

Для каждого ТСК АС выбирается один из типовых проектов компонента СЗИ. Осуществляется привязка проектов к условиям ТСК. Производится объединение всех компонентов в СЗИ.

Целесообразно применять, когда: Требования к ЗИ не очень высокие. Строго определенная структура АС. Архитектура АС близка к одной из типовых. Требования и/или условия защиты в различных ТСК различны.

3. Использование функционально-ориентированных компонентов СЗИ.

Для каждой группы компонентов АС выбираются по одному из типовых функционально ориентированных компонентов СЗИ. Осуществляется привязка проектов к условиям группы. Производится объединение компонентов в подсистему СЗИ. Все подсистемы объединяются в СЗИ.

Целесообразно применять, когда: Требования к ЗИ не очень высокие. В АС выделяются компактно расположенные компоненты. Требования и условия защиты в различных частях АС различны.

4. Разработка индивидуального проекта СЗИ, для реализации которого создаются индивидуальные средства защиты.

Разрабатывается проект индивидуальной СЗИ. Разрабатываются средства для реализации проекта. Осуществляется наладка СЗИ.

Целесообразно применять, когда: Требования к ЗИ очень высокие. Защищаемая информация имеет особую важность. АС является уникальной.

5. *Разработка индивидуального проекта с использованием ТПР по средствам защиты.*

Разрабатывается проект индивидуальной СЗИ, для реализации которого используются ТПР по основным средствам защиты.

Целесообразно применять, когда: Требования к ЗИ очень высокие. АС имеет ярко выраженные особенности.

6. *Использование ТПР по семирубежной модели.*

На плане территориального размещения АС намечаются рубежи защиты. Для каждого рубежа выбирается один из типовых проектов подсистемы СЗИ. Осуществляется привязка проектов к условиям каждого реального рубежа. Все подсистемы объединяются в СЗИ.

Целесообразно применять, когда: Требования к ЗИ не слишком высокие. Компоненты АС распределены на значительной территории. АС имеет сетевую структуру. Требования и условия защиты в различных компонентах АС различны.

1. 1 Лекция №12 (2 часа).

Тема: Методы и методики проектирования КСИБ от НСД.

1.1.2 Вопросы лекции:

Концептуальные основы построения защиты информации от несанкционированного доступа в вычислительной системе. Основы проектирования КСИБ от несанкционированного доступа.

1.1.2 Краткое содержание вопросов:

Для сетей, кроме защиты самой АСОИ (автоматизированной системы обработки информации) необходимо защитить и каналы связи.

Принимая во внимание, что информация в сети постоянно обновляется, а также и то, что на каналах связи, в отличие от элементов сети нарушитель ничем не рискует, особенно при пассивном перехвате информации, прочность защиты здесь должна быть особенно высокой.

От активного вмешательства нарушителя в процесс обмена информацией между элементами сети должна быть применена система обнаружения и блокировки несанкционированного доступа, но и при этом риск нарушителя по-прежнему не высок, т.к. у него и в этом случае, по причине сложности определения его пребывания, остается достаточно времени на то, чтобы отключиться и уничтожить свои следы. Поэтому в качестве сходной модели потенциального нарушителя высокой квалификации такой подход поможет защититься также от нарушителей, являющихся законными пользователями данной сети. Кроме того это позволит защитить системные отношения между элементами сети.

Поскольку физически каналы связи в сети защитить не представляется возможным, целесообразно строить защиту информации и сопровождающих ее служебных признаков на основе специальных криптографических преобразований, т.е. на основе самой информации, а не на ресурсах сети.

Такой основой должна быть кодограмма сообщений, которой обмениваются между собой элементы сети. Целостность этой кодограммы и содержащаяся в ней информация должны быть защищены от несанкционированного доступа.

Данная кодограмма, как правило, содержит адрес получателя, заголовок, информацию отправителя, концевик, адрес отправителя, исходящий номер и время отправления. В пакетном режиме добавляется еще и номер пакета, поскольку сообщение разбивается на пакеты, которые на объекте-получателе должны быть собраны в одно сообщение, чтобы оно приобрело первоначальный вид. Для синхронизации, приема и обработки кодограммы, в нее включаются признаки кадра. Кадр содержит информационное поле, а также заголовок и концевик, присваиваемый протоколом. Заголовок содержит служебную информацию, используемую протоколом канального уровня принимающей станции и служащую для идентификации сообщения правильного приема кадров, восстановления и повторной передачи в случае ошибок. Концевик содержит проверочное поле, служащее для коррекции и исправления ошибок.

Для обеспечения передачи блоков данных от передающей станции приемной кодограмма содержит признаки маршрута. Все эти и другие составляющие кодограммы формулируются на основе известной семиуровневой модели протокола взаимодействия открытых систем.

Анализ проведенных исследований в области безопасности информации в вычислительных сетях, позволяет взять за основу следующие требования, которые должны быть конечной целью при создании средств ее защиты.

После того, как соединение между абонентами вычислительной сети установлено, необходимо обеспечить четыре условия:

Получатель сообщения должен быть уверен в истинности источника данных.

Получатель сообщения должен быть уверен в истинности полученных данных.

Отправитель должен быть уверен в доставке данных получателю

Отправитель должен быть уверен в истинности доставленных получателю данных

При этом предполагается, что выполнение этих условий включает защиту от следующих активных вторжений нарушителя:

Воздействие на поток сообщений (изменение, удаление, задержки, переупорядочивание, дублирование и посылка ложных сообщений)

Воспрепятствие передачи сообщений

Осуществление ложных соединений

Однако, приведенные выше 4 условия не включают защиту от пассивных вторжений:

Чтение содержания сообщения

Анализ трафика и идентификаторов абонентов сети.

Отправитель и получатель должны в данной сети иметь полномочия на обмен друг с другом.

Для полноты постановки задачи к указанным 4-м условиям нужно добавить еще 4:

Отправитель и получатель должны быть уверены, что никому, кроме них и специального посредника факт передачи сообщения между ними не известен.

Отправитель и получатель должны быть уверены, что с доставленной информацией в сообщении никто кроме них не ознакомился.

Получатель должен быть уверен, что отправитель — это то лицо, за которое он себя выдает.

Отправитель должен быть уверен, что получатель — то лицо, которое ему необходимо для передачи сообщения.

Данные требования рассчитаны на защиту от квалифицированного нарушителя-профессионала. Защищать будем кодограмму. Нарушителю доступна вся кодограмма, включая служебные признаки.

Единственный метод защиты — это криптографические преобразования.

Один из методов должен быть таким, чтобы в кодограмме сохранились некоторые адреса и служебные признаки в открытом виде, поскольку всю кодограмму преобразовывать нецелесообразно по причине невозможности ее дальнейшей обработки.

Таким методом может быть использование механизма формирования цифровой подписи на базе несимметричных алгоритмов шифрования.

Для того, чтобы обеспечить возможность контроля и разграничения доступа, необходимо для всех участников обмена информацией помимо условных номеров присвоить переменные идентификаторы в виде паролей, которые могут передаваться в открытом виде, и подлинность которых будет обеспечиваться механизмом цифровой подписи.

Тем абонентам, которым присвоены соответствующие полномочия, должны быть предоставлены соответствующие значения паролей и закрытых ключей шифрования.

Стойкость защитного механизма определяется стойкостью к подбору примененного секретного ключа в количестве времени, затрачиваемого нарушителем на эту работу. Если оно составляет величину, превышающую время жизни защищаемой информации, то прочность этой преграды равна 1. При этом обратим внимание на существенную разницу во времени жизни самого сообщения и его служебных частей. Само сообщение в зависимости от назначения автоматизированных систем обработки данных может сохранять цену десятки лет, а его служебные части — не более 10 минут. Это позволяет существенно увеличить быстродействие шифрования и , может быть, даже упростить его для служебных частей. Такой большой набор процедур может вызвать сомнения у разработчиков по поводу реальности воплощения этой идеи из-за возможного увеличения времени обработки кодограммы. Однако, даже если это и случится, повышение безопасности информации стоит того. При реализации системы контроля и разграничении доступа в АСУ, потребуется также организовать систему сбора в сети сигналов, несовпадение кодов паролей, систему управления и распределения ключей шифрования информации и организационные мероприятия по безопасности информации.

1. 1 Лекция №13 (2 часа).

Тема: Методы и методики оценки КСИБ

1.1.3 Вопросы лекции:

Обзор методов и методик оценок уязвимостей. Метод оценки уязвимостей информации Хоффмана.

1.1.2 Краткое содержание вопросов:

Сегодня не существует общепринятых методов и методик оценки качества КСИБ, как не существует и общепринятого набора показател□ей качества функционирования КСИБ. Всякая оценка качества защиты информации каждый раз является актом творчества и разными авторами решается по-разному. При этом можно определить ряд факторов, которые крайне важно учитывать при оценке качества КСИБ.

1. Обеспечение информационной безопасности на практике происходит под воздействие большого числа случайных факторов, некоторые из которых систематизированы в ГОСТ Р 51275 99.

2. Существуют обстоятельства заранее неизвестные или казавшиеся несущественными при проектировании КСИБ, которые способны значительно снизить или даже полностью скомпрометировать предусмотренные проектом меры информационной безопасности.

3. Объективное подтверждение эффективности функционирования СЗИ является сложным, а иногда и вовс□е невозможным.

4. В вопросах обеспечения информационной безопасности, как впрочем и во многих других областях, нормативная база отстает от потребностей практики. В частности непроработанными остаются такие аспекты как система показател□ей информационной безопасности; система критериев, обеспечивающих оптимальный уровень безопасности и учитывающих стохастическую природу явлений и событий, которые возникают в процессе защиты информации, а также их экономическое содержание.

5. Проектирование и применение СЗИ объективно связаны с неизвестными событиями в будущем и вс□егда содержат элементы неопредел□енности. По мере реализации проекта неопредел□енность снижается, но никогда эффективность СЗИ не должна быть адекватно выражена и описана детерминированными показателями.

Исходя из вышеизложенных факторов, возможным способом определ□ения уровней гарантий безопасности бывают вероятностно-статистические методы, нашедшие широкое применение в практике обеспечения безопасности во многих прикладных областях.

Следует отметить, что в контексте оценивания СЗИ сам термин □□вероятность□□ имеет несколько различных значений. Наиболее часто встречаются два толкования этого слова, которые обозначаются сочетаниями □□объективная вероятность□□ и □□субъективная вероятность□□. Понятие □□объективная вероятность□□ (ее еще называют физической) вам должно быть хорошо знакомо - э □□ отношение общего числа благоприятных исходов к общему количеству испытаний при количестве испытаний, стремящемуся к бесконечности. Иначе говоря, это относительная частота появления какого-либо события в общем объёме наблюдений. Объективная вероятность определяется при анализе большого числа наблюдений, имевших место в прошлом или как следствие из модел□ей, описывающих некоторые процессы.

Под субъективной вероятностью принято понимать мера уверенности некоторого человека или группы людей (экспертов) в том, что данное событие действительно будет иметь место.

Субъективная вероятность должна быть формально представлена несколькими способами□

- вероятностным распредел□ением на множестве событий;
- бинарным отношением на множестве событий;
- описана математическим аппаратом нечетких множеств;
- описана функцией полезности на множестве альтернатив (с учетом предпочтений лица, принимающего решение). Возможны и другие способы представления субъективной вероятности.

По статистическим данным Национального отдел□ения ФБР США по компьютерным преступлениям, реальный уровень эффективности СЗИ недопустимо

низок. Так вероятность предотвращения несанкционированного доступа в информационную систему в среднем составляет около 0,12, а вероятность обнаружения нападения на корпоративные сети оценивается величиной 0,03–0,15. В то же время нормы безопасности, изложенные в соответствующих документах, имеют порядок 0,9.

1. 1 Лекция №14 (2 часа).

Тема: Аттестация АС по требованиям безопасности.

1.1.4 Вопросы лекции:

Положение об аттестации объектов информатизации по требованиям ИБ.Порядок проведения аттестации и контроля. Классификация АС и требования по защите информации.

1.1.2 Краткое содержание вопросов:

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа (Аттестат соответствия) подтверждается, что объект отвечает требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Состав нормативной и методической документации для аттестации конкретных автоматизированных систем (АС) определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемой АС. Перечень исходных данных приведен в заявке на аттестацию (см. положение по аттестации [1, 2]). Аттестат соответствия выдается владельцу АС на период, в течение которого обеспечивается неизменность условий функционирования системы и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое ПО, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Контролирование

Положением по аттестации предусмотрено три вида контроля:

Государственный контроль и надзор, инспекционный контроль за проведением аттестации проводится территориальным управлением ФСТЭК России как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных АС - периодически в соответствии с планами работы по контролю и надзору.

Органом по аттестации объектов информатизации, проводившим аттестацию АС, ежегодно - в соответствии с программой аттестационных испытаний.

Самоконтроль осуществляется службой безопасности учреждения, проводится периодически (не реже одного раза в год).

Контроль заключается в оценке:

соблюдения нормативных и методических документов ФСТЭК России;

работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

знаний и выполнения персоналом своих функциональных обязанностей в части за щиты информации.

В силу исторической направленности работ по аттестации на защиту государственной тайны данные работы явно перегружены утечками по техническим

каналам, что вызывает большие затраты и требования к специалистам по защите информации на местах. В частности, для прохождения учебного курса "Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам" слушателям необходимо иметь справку о допуске и предписание на выполнение задания "форма 16".

Не хватает также публичности информации об организациях, имеющих аттестат, а также актуальности и статуса действия этого сертификата. Согласно Положению ведение сводных информационных баз аттестованных объектов информатизации осуществляется ФСТЭК России или по ее поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов, но для бизнеПЗ-компаний более предпочтительным является вариант с публичным реестром аттестатов (или выписок из них), что позволит предприятиям выбирать себе подходящих партнеров.

В силу указанных причин для некоторых бизнеПЗ-компаний более привлекательной может быть сертификация в рамках российской аккредитации ISO. Данный вариант имеет большую международную направленность, а также считается менее зависимым от государственных структур.

Опыт зарубежных стран

Если обратиться к опыту других стран, в частности Германии, то немецкое Федеральное управление по ИТ-безопасности BSI (Bundesamt f?r Sicherheit in der Informati-onstechnik) разработало ряд стандартов (100-1, 100-2, 100-3) в области ИБ, по которым разработана схема сертификации как государственных, так и бизнеПЗ-компаний. Стандарты охватывают каталоги базовых требований, угроз, мер защиты, руководства по анализу рисков, инструментарий для самооценки соответствия требованиям. При этом, несмотря на отличие данных стандартов от стандартов ISO, по просьбе бизнеПЗ-компаний в добавление к собственной схеме сертификации была также разработана схема параллельного получения международного сертификата ISO/IEC 27001 при выполнении требований немецких стандартов.

Немецкое Федеральное управление по финансовому надзору BaFin (Bundesanstalt fur Finanzdienstleistungsauf-sicht) разработало ряд нормативных документов (Kon-TraG и MaRisk) для финансовых учреждений, на основе которых рекомендовало внедрение стандартов BSI.

В США в 2002 г. была принята Федеральная программа по ИБ FISMA (Federal Information Security Management Act), пришедшая на смену устаревшему Government Information Security Reform Act (GIS-RA). Данная программа распространяется не только на федеральные агентства, но и на любые коммерческие организации, работающие с ними. Каждое агентство должно разработать программу по ИБ, проводить периодически анализ рисков и на основе этого анализа выбирать соизмеримые ущербу средства контроля. Программа должна предусматривать такие меры, как реагирование на инциденты и обеспечение непрерывности выполнения ИТ-операций. Она предусматривает схемы аккредитации и сертификации, при этом была разработана специальная программа "ISO 27001 Harmonization Initiative" по гармонизации с международным стандартом ISO/IEC 27001. В настоящий момент завершена первая фаза программы, в рамках которой уже разработано более 10 стандартов и руководств по ИБ.

Ежегодно каждое агентство обязано отчитываться перед Конгрессом об адекватности и эффективности используемой программы, а также проводить независимый аудит ИБ на предмет ее эффективности. Для поощрения данных инициатив была

разработана специальная ежегодная премия eGov Awards.
Таким образом, необходимо отметить назревшие перемены в российской программе аттестации. Основные направления совершенствования, на которые следует обратить внимание, лежат в области гармонизации с международными стандартами, а также в области интересов коммерческих предприятий и компаний.

Важным этапом при проектировании автоматизированной системы в защищенном исполнении является модель нарушителя как одного из аспектов требований к безопасности объекта информатизации. Выбранная модель отчасти определяет класс защищенности системы, жесткость предъявляемых требований как к аппаратно-программным средствам защиты информации, так и к организационно-режимным мерам. Именно выбор средств защиты может ускорить дальнейшую аттестацию системы.

Так, наличие сертификата ФСТЭК России у средства защиты информации исключает необходимость работы по его испытаниям в испытательных центрах в сфере сертификации средств защиты информации по требованиям ИБ при проведении аттестации объекта информатизации.

Спрос на услуги по аттестации информационных систем на соответствие требованиям российского законодательства формируется главным образом за счет государственных организаций, для которых наличие Аттестата соответствия во многих случаях является обязательным требованием. Аттестат соответствия является официальным подтверждением эффективности мер и средств защиты информации, используемых на конкретном объекте информатизации, и выдается по результатам комплексного обследования организационной и информационной структуры объекта, а также проведения соответствующих испытаний. При этом проводить аттестацию объекта может лишь уполномоченный орган по аттестации - организация, аккредитованная в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00.

В какой-то степени здесь можно провести аналогию с завоевывающими сейчас все большую популярность услугами по сертификации на соответствие требованиям международных стандартов, в частности ISO/IEC 27001. Основным этапом в данном случае также является обследование (аудит), однако объектом проверки при этом выступает только система управления информационной безопасностью (СУИБ). Сертификационный аудит проводится органом по сертификации, имеющим соответствующую аккредитацию

1. 1 Лекция №15 (2 часа).

Тема: Особенности эксплуатации КСИБ на объекте защиты

1.1.1 Вопросы лекции:

Основные меры по защите информации. Основные требования и рекомендации по защите служебной тайны и персональных данных.Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС.

1.1.2 Краткое содержание вопросов:

Особенности эксплуатации КСИБ на объекте защиты, организационно-функциональные задачи службы безопасности.
Эксплуатация – стадия жизненного цикла изделия (системы) с момента принятия его эксплуатирующей организацией от изготовителя, с базы хранения (склада) или из

ремонтного предприятия до списания.
Эксплуатация включает в себя следующие этапы:
– ввод в эксплуатацию;
– приведение в установленную степень готовности к использованию по назначению;
– поддержание в установленной степени готовности к этому использованию (техническое обслуживание, ремонт);
– использование по предназначению;
– хранение;
– транспортировка;
– списание.
Ввод КСИБ в эксплуатацию включает в себя следующие мероприятия:
– подготовительные работы;
определение состава комиссии по освидетельствованию технических средств информатизации;
изучение товарно-транспортных документов.
– контроль и приемка системы (изделий), поступившей от производителя, базы хранения (склада) или от другой организации (поставщика) эксплуатирующей организацией:
внешний осмотр и проверка соответствия количества, массы и габаритов упаковочных мест сопроводительной документации, а также состояния тары, пломб, печатей;
вскрытие упаковок и внешний осмотр изделий;
изучение формуляров комплекса и его комплектующих изделий;
проверка комплектности полученного оборудования;
развертывание полученного оборудования на месте эксплуатации, подключение вспомогательных и взаимодействующих устройств;
контроль работоспособности во всех штатных режимах, измерение основных параметров;
составление акта приема по установленной форме;
запись в формуляре о приемке с указанием номера и даты акта.
– закрепление оборудования за должностным лицом или должностными лицами.
издание приказа о закреплении;
запись в формуляре изделия о закреплении.
Функциональные задачи службы защиты информации
Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям:
1. Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема имеет своего сотрудника группы безопасности.
2. Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.
3. Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты набор данных, ужесточение защиты в случае необходимое, а также координирование работы с другими администраторами.
4. Руководитель группы. В его обязанности вход разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных, оборудования и программного обеспечения, контроль за выполнением плана восстановления и последующее руководство административными группами в подсистемах ИС (при децентрализованном управлении)
В небольших организациях функции руководителя службы обычно выполняет либо глава

фирмы, либо его заместитель.
Количественный состав службы безопасности ограничен и зависит, прежде всего, от возможностей сам фирмы. Возможны различные варианты состава так группы. Кроме того, перечень необходимых знаний навыков, а также функциональных обязанностей входящих в группу защиты информации может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной ИС.
Организационные основы и принципы деятельности службы
Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.
Принципы организации Службы безопасности
Принципы организации СБ выражают основополагающие требования к стратегии и тактике, организации и осуществлению мероприятий по защите жизненно важных интересов предприятия, концентрируют опыт успешного решения задач в этой сфере деятельности.
1. Законность. Меры безопасности предприятия разрабатываются на основе норм права в пределах определенной данным типовым положением компетенции с применением всех дозволенных Законом методов обнаружения и пресечения правонарушений в сфере безопасности.
2. Самостоятельность и ответственность. СБ располагают всеми необходимыми для своей деятельности видами ресурсов, при использовании которых обеспечивается строгое соответствие производимых затрат и достигаемых результатов, материальная ответственность инициаторов и исполнителей соответствующих мероприятий за результаты своей деятельности.
3. Экономическая целесообразность и прибыльность. Мероприятия по обеспечению безопасности предприятия не должны приводить к ухудшению экономических показателей деятельности предприятия, а стабильность его прибылей является главным критерием оценки качества работы СБ, определения размеров материального вознаграждения их сотрудников.
4. Специализация и профессионализм. Кадровый состав подразделений безопасности специализируются по направлениям комплексного обеспечения безопасности предприятия. Профессиональная подготовка сотрудников СБ предприятия должна позволять широко использовать научные достижения и передовой опыт организации работ обеспечению безопасности объектов. В противном случае противодействия ЗЛ становятся проблематичными.
5. Программно-целевое планирование. Деятельность СБ предприятия по обеспечению безопасности осуществляется на основании комплексной программы и разрабатываемых на ее основе планов работ и отдельных мероприятий.
6. Взаимодействие и координация. Меры безопасности осуществляются на основе взаимодействия скоординированности усилий всех заинтересованных подразделений предприятия, а также установления необходимых связей с внешними организациями (органами государственного управления, правоохранительными органами, другими предприятиями и фирмами). Деятельность в сфере безопасности не должна нарушать нормальных условий работы предприятия на других направлениях.
7. Гласность в сочетании с необходимой конспирацией. Руководящие органы предприятия регулярно «формируют своих сотрудников о мероприятиях по обеспечению безопасности. В оправданных ситуациях меры безопасности могут носить конспиративный характер. Конспиративность мер безопасности предполагает специальную организацию контроля руководящих органов СБ предприятия за их применением, соблюдением необходимых правил-процедур

1. 1 Лекция №16 (2 часа).

Тема: Модели защиты информации.

1.1.1 Вопросы лекции:

Основные модели защиты информации. Реализация ядра безопасности.

1.1.2 Краткое содержание вопросов:

Существует множество моделей защиты информации. Но все они являются модификациями трёх основных: дискреционной, мандатной и ролевой.

Дискреционная модель обеспечивает произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей – субъектов, которые осуществляют доступ к информации, пассивных сущностей – объектов, содержащих защищаемую информацию и конечного множества прав доступа, означающих полномочия на выполнение соответствующих действий. Принято считать, что все субъекты одновременно являются и объектами (обратное неверно). Поведение системы характеризуется текущим состоянием, текущее состояние характеризуется тройкой множеств: субъектов, объектов и матрицы прав доступа, описывающей текущие права доступа субъектов к объектам.

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных учреждениях многих стран. Всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, назначается специальная метка, получившая название уровень безопасности. Все уровни безопасности упорядочиваются по доминированию. Контроль доступа основывается на двух правилах:

1. Субъект имеет право читать только те документы, уровень безопасности которых ниже или равен уровню субъекта.
2. Субъект имеет право заносить информацию только в документы, уровень которых выше или равен уровню субъекта.

Ролевая модель представляет собой существенно усовершенствованную дискреционную модель, однако её нельзя отнести ни к дискреционным, ни к мандатным моделям, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль

Моделирование системы состоит в построении некоторого ее образа, соответствующего (с точностью до целей моделирования) исследуемой системе, и получения с помощью сформированной модели необходимых характеристик реальной системы.

Классификация моделей может быть осуществлена по совокупности трех критериев:

а) Способ моделирования

Аналитический - модель представляет собой совокупность аналитических и (или) логических зависимостей, позволяющих определить необходимые характеристики путем проведения вычислений по указанным зависимостям.

Статистический - моделируемая система представляется в виде некоторого аналога, отражающего для определяемых характеристик зависимости реальной системы. Определение значений данных характеристик осуществляется путем многократной имитации реализации зависимостей характеристик от существенно значимых параметров реальной системы и внешней среди и статистической обработки совокупности получаемых результатов.

б) Характер системы

Детерминированные - все зависимости между подлежащими определению на модели значениями характеристик моделируемой системы и влияющими на них параметрами системы и внешней среды строго определены.

Стохастические - на зависимости оказывают существенное влияние случайные факторы.

в) Масштаб моделирования

Общие - строятся с целью определение значений некоторых обобщенных характеристик моделируемых систем.

Частные - с целью определения частных, локальных характеристик системы.

Поскольку на процессы защиты большое влияние оказывают случайные факторы, то в подавляющем большинстве эти модели стохастические, поэтому выделяют 4 вида моделей:

аналитические общие

аналитические частные

статистические общие

статистические частные

Методы моделирования - описание структуры и процессов функционирования системы и имитация процессов функционирования систем.

Описание структуры системы может быть осуществлено методами теории множеств и теории графов и должно содержать перечень всех ее существенно значимых элементов, взаимосвязи между элементами и отображать характер этих взаимосвязей.

Для описания процессов функционирования стохастических систем необходимы средства отображения влияния случайных факторов. Такие средства содержатся в методах статистических испытаний (Монте-Карло), теории массового обслуживания, теории вероятностных автоматов и др.

1. 1 Лекция №17 (2 часа).

Тема: Реализация системы управления доступом.

1.1.1Вопросы лекции:

Особенности выбора СКУД для конкретных объектов. Основные компоненты СКУД.

Устройство идентификации доступа. Типовые варианты СКУД.

1.1.3 Краткое содержание вопросов:

В некоторых случаях системы безопасности, которые называют интегрированными, таковыми не являются, поскольку в них реализована лишь часть базовых функций подсистем. Кроме того, зачастую возникает проблема несовместимости

средств и систем различных производителей. Причина тому - отсутствие нормативной документации, содержащей требования по интеграции подсистем.

Основные типы технических средств и систем

При построении интегрированной системы охраны (ИСО) объекта возникает проблема выбора базового компонента (соответствующей подсистемы), обеспечивающего путем наращивания его функциональных возможностей решение всего необходимого круга задач.

Исходя из перечня функций, реализуемых системой охраны, можно определить номенклатуру применяемых технических средств и систем (см. таблицу).

СКУД как основа ИСО

Анализируя данные, представленные в таблице, видно, что система контроля и управления доступом (СКУД) может быть выбрана основополагающей (базовой) подсистемы, поскольку при помощи нее реализуются все функции ИСО.

Действительно, современная СКУД является сложным аппаратно-программным комплексом, предназначенным не только для осуществления санкционированного доступа на объект, но и для решения других проблем, например, обнаружение запрещенных предметов (оружия, взрывчатых веществ и радиоактивных материалов и т.п.). Применение современных информационных технологий предоставляет пользователю такой системы множество дополнительных сервисных функций, среди которых: контроль местоположения персонала, передача информационных сообщений, учет рабочего времени и т.д. При построении современных СКУД применяются самые передовые технологии и технические решения, обеспечивающие высокую надежность и скорость передачи информации.

СКУД + охранная сигнализация

В архитектуре построения современных СКУД можно выделить некоторые важные особенности.

Так, элементы СКУД применяются практически везде, где установлены средства охранной сигнализации. Очень часто системы охранной сигнализации и СКУД взаимно дополняют друг друга при решении задач по охране находящихся в помещениях материальных и информационных ценностей. Современные СКУД позволяют контролировать состояние нескольких средств обнаружения (извещателей) и передавать сигналы о тревожных ситуациях на соответствующие пульты управления (ПУ). Примером может служить постановка (снятие) помещения под охрану (с охраны) при интеграции функций СКУД и системы охранной сигнализации. В простейшем случае первый из вошедших санкционированных пользователей снимает помещение с охраны, а последний выходящий ставит его под охрану. Аналогично могут решаться вопросы интеграции с лифтами, инженерными системами объекта и т.п.

Организация пультов управления

Современные СКУД позволяют создать развитую систему охраны с наличием разнообразных ПУ. Очевидно, что ПУ, установленный у дежурного по КПП, значительно отличается по набору функциональных возможностей и отображаемой информации от ПУ, установленного у оператора, осуществляющего контроль работы той части СКУД, которая обеспечивает доступ в охраняемые помещения. В то же время в других системах, входящих в комплекс технических средств охраны, такого различия, как правило, не возникает. Зачастую ПУ в таких системах являются унифицированными, а вся нформация о состоянии средств, входящих в систему, и необходимые органы управления

объединяются на одном, центральном ПУ для возможности общей оценки развития ситуации и оптимизации действий сил охраны. Если все же возникает необходимость разделить информацию, предоставляемую операторам, возможность организации локальных и центрального ПУ, заложенная и реализованная в СКУД, является незаменимой.

Базы данных

Отдельно следует отметить наличие развитой базы данных (БД), которая отличает СКУД от других охранных систем. Проводя анализ хранимой в ней информации, можно сделать вывод о том, что ее доработка потребует значительно меньших вложений для дальнейшей доработки, чем БД, например, системы охранной сигнализации. Следует также отметить, что в соответствии с требованиями ГОСТ Р 51241 в таких БД уже должны быть учтены требования по разграничению доступа к информации со стороны различных пользователей.

Пропускные устройства

Важной составной частью СКУД являются пропускные устройства (УПУ). При выборе типа УПУ пользователь имеет возможность решить несколько задач. Во-первых, УПУ могут выполнять функцию обнаружения в случае попытки их несанкционированного преодоления. Во-вторых, УПУ шлюзового типа с полным перекрытием дверного проема решают задачу задержания несанкционированных пользователей или лиц, пытающихся пронести запрещенные предметы. Учитывая, что УПУ в ряде случаев представляют собой инженерное сооружение, они также могут выполнять функцию сдерживания (задержки).

Дополнительные функции

Требования, предъявляемые к универсальным СКУД, которые изложены в ГОСТ Р 51241, позволяют говорить и о других важных возможностях системы, а именно:

· выдача информации работникам службы безопасности о выполнении действий под принуждением (реализация функции тревожно-вызывной сигнализации);

· интеграция с системами охранной, пожарной сигнализации и средствами видеонаблюдения;

· управление дополнительными устройствами (освещение, вентиляция, лифты, технологическое оборудование и т.д.);

· подключение переговорных устройств.

Проблемы интеграции

Все вышеизложенное свидетельствует о том, что правильно спроектированная СКУД может стать основой построения ИСО.

Однако при создании интегрированных систем между производителями и потребителями зачастую возникают коллизии, вызванные отсутствием необходимой нормативной документации, определяющей требования к интеграции. Это приводит к целому ряду проблем, которые можно разделить на две основные группы: терминологические и технические. К сожалению, в ряде случаев даже известные производители не всегда корректно используют понятие "интегрированная система". Поскольку термин "интеграция" в данном контексте можно рассматривать как слияние различных систем в единое целое, то, по мнению автора, под интегрированной системой следует понимать только такую систему, которая обеспечивает полную реализацию всех базовых функций, присущих двум или более входящим в ее состав функциональным подсистемам.

Системы, не относящиеся к интегрированным

Как уже отмечалось, наиболее часто на аппаратном и/или программном уровне объединяются подсистемы контроля и управления доступом и охранной сигнализации. Однако далеко не все системы, называемые интегрированными, могут быть отнесены к данному классу. В отдельных случаях в СКУД добавляют отдельные элементы системы охранной сигнализации (например, прием и представление оператору информации от отдельных типов средств обнаружения). В других - в систему охранной сигнализации добавляют элементы контроля и управления доступом (к примеру, в ряде случаев автоматическая постановка/снятие помещения под охрану/с охраны, совмещенная с разблокировкой/блокировкой входа выдается как контроль и управление доступом). В некоторых системах присутствует только часть функций как систем охранной сигнализации, так и контроля и управления доступом. Очевидно, что во всех приведенных примерах нельзя говорить об интегрированных системах, поскольку не реализуется базовый набор функций, присущий обеим функциональным подсистемам. В ряде случаев можно говорить только о системах, имеющих расширенный набор функций.

Основные базовые функции

К сожалению, в рамках одной статьи невозможно рассмотреть полный перечень базовых функций рассматриваемых систем, однако очевидно, что система охранной сигнализации должна обеспечивать:

· возможность работы с различными типами средств обнаружения, устанавливаемых как внутри, так и снаружи помещений, при наличии как минимум соответствующей защиты входных цепей;

· электропитание средств обнаружения, в том числе удаленных на значительное расстояние;

· дистанционный контроль их работоспособности;

· функционирование в широком диапазоне внешних воздействующих факторов, в том числе в части электромагнитной совместимости;

· реализацию различных тактик постановки/снятия под охрану/с охраны и т.д.

Современная СКУД в свою очередь должна:

· обеспечивать контроль и управление доступом на различных типах контрольно-пропускных пунктов (пешеходных, автомобильных, железнодорожных), а также в категорированные помещения объекта;

· исключать пронос/провоз запрещенных предметов (оружия, взрывчатых веществ и т.п.);

· задерживать потенциальных нарушителей;

· поддерживать различные способы удостоверения проходящих лици т.д.

Необходимость создания единого стандарта

Резюмируя выше сказанное, можно отметить, что только системы, реализующие все перечисленные и некоторые другие базовые функции, могут быть отнесены к интегрированным системам управления доступом и охранной сигнализации. Очевидно, что для обеспечения единства понимания необходимо разработать национальный стандарт (или группу стандартов), в котором должны быть определены базовые требования, предъявляемые к различным функциональным подсистемам, входящим не только в систему охраны, но и в другие системы, относящиеся к комплексной системе безопасности.

Другая проблема, возникающая при интеграции систем и средств, выпускаемых различными производителями, это их совместимость. Разработка и введение в действие единого стандарта, определяющего вопросы технической, информационной, энергетической, конструктивной и иных видов совместимости, позволят значительно упростить решение возникающих у потребителей проблем.

В связи с вступлением в силу Федерального закона "О техническом регулировании" необходимо пересмотреть нормативную документацию, устанавливающую требования к различным средствам и системам, в том числе обеспечивающим безопасность. Необходимо объединить усилия производителей и потребителей для разработки комплекта документов, устанавливающих оптимальную систему требований, что позволит сделать рынок более цивилизованным и обеспечит в итоге повышение уровня безопасности.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

2.1 Практическое занятие №1 (2 часа).

Тема: «Введение в предмет»

2.1.1 Вопросы к занятию:

1. Основные понятия и определения АС.

2.1.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.4 Практическое занятие №2-3 (4 часа).

Тема: «Современные тенденции в программной инженерии»

2.4.1 Вопросы к занятию:

1. Основные проблемы современных проектов
2. «Быстрая разработка ПО»

2.4.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.5 Практическое занятие №3-4 (2 часа).

Тема: «Нормативно-методическое обеспечение создания АС»

2.5.1 Вопросы к занятию:

1. Нормативно-методическое обеспечение АС.
2. Международные стандарты.
3. Стандарты Российской Федерации.
4. Стандарты организации-заказчика.

2.5.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.6 Практическое занятие №5-6 (4 часа).

Тема: «Стандарт жизненного цикла АС»

2.6.1 Вопросы к занятию:

1. Основные процессы жизненного цикла АС.
2. Вспомогательные процессы жизненного цикла АС.
3. Взаимосвязь между стандартными процессами и стадиями.

2.6.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.7 Практическое занятие №7 (2 часа).

Тема: «Модели жизненного цикла АС»

2.7.1 Вопросы к занятию:

1. Модель ЖЦ АС.

2. Каскадные модели ЖЦ АС.
3. Итерационные модели ЖЦ АС.
4. Эволюционная модель ЖЦ АС.

2.7.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.10 Практическое занятие №8-9 (4 часа).

Тема: «Оценка процессов создания АС»

2.10.1 Вопросы к занятию:

1. Понятие зрелости процессов создания АС.
2. Модель оценок зрелости.

2.10.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.11 Практическое занятие №10 (2 часа).

Тема: «Общие принципы проектирования АС»

2.11.1 Вопросы к занятию:

1. Структурный подход к анализу и проектированию АС.
2. Визуальное моделирование.
3. Языки моделирования.

2.11.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.12 Практическое занятие №11-12 (4 часа).

Тема: «Методология IDEF»

2.12.1 Вопросы к занятию:

1. Структурный синтез систем.
2. Методологии структурного синтеза.
3. IDEF0.
4. IDEF1.
5. IDEF1x.
6. IDEF2.
7. IDEF3.
8. IDEF4.
9. IDEF5.

2.12.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.13 Практическое занятие №13 (2 часа).

Тема: «Методология eEPC»

2.13.1 Вопросы к занятию:

1. Особенности методологии eEPC.
2. Нотация методологии eEPC.

2.13.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.16 Практическое занятие №14 (2 часа).

Тема: «Постановка проблемы комплексного обеспечения информационной безопасности АС»

2.16.1 Вопросы к занятию:

1. Понятия «комплексности» и «системности».
2. Основополагающие меры комплексной безопасности АС.

2.16.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.17 Практическое занятие №15 (2 часа).

Тема: «Особенности проектирования на современном уровне и синтез КСИБ»

2.17.1 Вопросы к занятию:

1. Основные подходы при проектировании.
2. Общая характеристика проблемы синтеза систем защиты.
3. Типовая структура КСЗИ от несанкционированного доступа.

2.17.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.18 Практическое занятие №16-17 (4 часа).

Тема: «Методы и методики проектирования КСИБ от НСД»

2.18.1 Вопросы к занятию:

1. Концептуальные основы построения защиты информации от несанкционированного доступа в вычислительной системе.
2. Основы проектирования КСИБ от несанкционированного доступа.

2.18.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.19 Практическое занятие №18 (2 часа).

Тема: «Методы и методики оценки КСИБ»

2.19.1 Вопросы к занятию:

1. Обзор методов и методик оценок уязвимостей.
2. Метод оценки уязвимостей информации Хоффмана.

2.19.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.22 Практическое занятие №19 (2 часа).

Тема: «Особенности эксплуатации КСИБ на объекте защиты»

2.22.1 Вопросы к занятию:

1. Положение об аттестации объектов информатизации по требованиям ИБ.
2. Порядок проведения аттестации и контроля.
3. Классификация АС и требования по защите информации.

2.22.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.23 Практическое занятие №20-21 (4 часа).

Тема: «Аттестация АС по требованиям безопасности»

2.23.1 Вопросы к занятию:

4. Положение об аттестации объектов информатизации по требованиям ИБ.
5. Порядок проведения аттестации и контроля.
6. Классификация АС и требования по защите информации.

2.23.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.24 Практическое занятие №22 (2 часа).

Тема: «Модели защиты информации»

2.24.1 Вопросы к занятию:

1. Основные модели защиты информации.
2. Реализация ядра безопасности.

2.24.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.

2.24 Практическое занятие №23 (2 часа).

Тема: «Реализация системы управления доступом»

2.24.1 Вопросы к занятию:

1. Особенности выбора СКУД для конкретных объектов.
2. Основные компоненты СКУД.
3. Устройство идентификации доступа.
4. Типовые варианты СКУД.

2.24.2 Краткое описание проводимого занятия:

Практическое занятие проводится в формах диспута и опроса по вопросам занятия.