V.L. Yevseyev, V.I. Korolev

Conceptual Designing Of Information Security. The Base Of The Discipline

Keywords: conceptual designing, system engineering, information security

The article reflects the conceptual design as a stage of the system engineering. The must to introduce the discipline «Conceptual designing of information security» is justified. The discipline is positioned in the structure of the educational program of higher professional education. The discipline is structured and its content is described.

В.Л. Евсеев, В.И. Королёв

КОНЦЕПТУАЛЬНОЕ ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. БАЗА УЧЕБНОЙ ДИСЦИПЛИНЫ

Концептуальное проектирование как профессиональный стандарт квалификации по обеспечению информационной безопасности

Концептуальное проектирование – стадия системной инженерии, на которой принимаются архитектурные, структурные, технические и организационные решения, определяющие последующий облик системы, проводится исследование принимаемых решений и их предварительное общесистемное согласование со всеми заинтересованными сторонами (стейкхолдерами)[4] .

Постоянное и существенное усложнение систем в условиях современного развития общества в любой области деятельности (экономика, техника, информатизация, социальные проблемы и т.д.) предопределило стадию концептуального проектирования систем как неотъемлемую часть их жизненного цикла, **предмет профессиональной подготовки**. Такое положение подтверждается повышенным вниманием, которое уделяет ИСО/МЭК созданию технических требований, стандартов, методических материалов по данному направлению[2, 3], активным развитием практики.

Концептуальное проектирование в области *информационной безопасности*(ИБ) приобрело высокую актуальность ввиду того, что применение традиционных детерминированных методов синтеза систем обеспечения информационной безопасности (СОИБ) выявило ограничения при их использовании. Основанное на этих методах проектирование частоне предоставляет возможность построения комплексных, интегрированных и эффективных моделей проектируемых систем, предназначенных для обеспечения ИБ при функционировании *автоматизированных систем* (АС) в сложных кибернетических средах. При этом под *кибернетическими средами*(КС) понимается совокупность средств, технологий и информационных ресурсов реализации самих АС как информационно-функциональных приложений обеспечения деятельности организаций и предприятий, реализации бизнес-процессов, а также средств и технологий, образующих инфраструктурные технологические системы. Инфраструктурные технологические системы по своей сущности являются информационно-телекоммуникационными и организационно-техническими объектами и системами, образующими среду обеспечения функционирования АС.

Данные предпосылки позволяют утверждать, что обладание знаниями и практикой концептуального проектирования информационной безопасности должно стать одним из важнейших факторов оценки профессионализма специалистов в области обеспечения информационной безопасности, профессиональным стандартом высокой ква-

лификации, а сама дисциплина концептуального проектирования ИБ – предметом изучения при подготовке этих специалистов.

Цели и задачи учебной дисциплины

Дисциплина «Концептуальное проектирование информационной безопасности» реализует требования Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) выпускника «магистр») [1] в отношении объекта профессиональной деятельности: методы и средства проектирования систем, средств и технологий обеспечения информационной безопасности объектов информатизации.

Цели дисциплины – изложение основных понятий, подходов и методов проектирования СОИБ в сложных кибернетических средах на концептуальном уровне, ознакомление с механизмами и моделями интеграции средств и технологий обеспечения информационной безопасности в системную архитектуру автоматизации/информатизации объекта, структурная и архитектурная компиляция защищённой кибернетической среды.

В соответствии с ФГОС п. 4.4 [1]**миссия** учебной дисциплины – обеспе6чение решения профессиональной задачи с профильной направленностью проектная деятельность: «Концептуальное проектирование сложных систем, комплексов средств и технологий обеспечения информационной безопасности».

Задачи дисциплины:

- раскрытие содержания базовых понятий концептуального проектирования сложных систем и решений;
- ознакомление с подходами и методологией работы со смыслами при принятии решений в размытых предметных областях;
- освоение аппарата системного анализа и системной инженерии, методов морфологического анализа объектов, структурного анализа технических систем, композиционного анализа и архитектурного подхода к проектированию информационно-технологической инфраструктуры информационных систем;
- обоснование и постановка парадигмы совмещения жизненных циклов сложных информационных систем и СОИБ для них, прежде всего, на этапе проектирования с учётом совершенствования традиционных методов проектирования СОИБ;
- рассмотрение современных сложных кибернетических сред и архитектур построения инфраструктуры систем обработки и передачи информации, требующих защищённого исполнения и практического применения методов концептуального проектирования при создании СОИБ;
- изучение форм, методов и моделей получения и представления результатов концептуального проектирования СОИБ в сложных кибернетических средах в зависимости от целевых функций проектирования;
- освоение подходов к планированию создания и методов структурного построения концепций СОИБ как компонентов систем обработки и передачи информации, подходов к экономической оценке принимаемых решений.

Поставленные цели и задачи определяют дисциплину «Концептуальное проектирование информационной безопасности» как неотъемлемую составную часть профессиональной подготовки в соответствии с ФГОС 090900 «Информационная безопасность».

Место учебной дисциплины в структуре основной образовательной программы высшего профессионального образования

Дисциплина «Концептуальное проектирование информационной безопасности» должна быть отнесена к базовым дисциплинам профессионального цикла. Она является необходимым элементом в обучении, обеспечивающим формирование современного профессионального подхода к принятию решений в размытых предметных областях и проектированию сложных систем в области ИБ. Для успешного освоения дисциплины необходимо владеть знаниями, умениями и навыками, сформированными в процессе изучения дисциплин общенаучного цикла, математического естественнонаучного модуля и профессионального цикла:

- «Экономика и управление»,
- «Современная философия и методология науки»,
- «Математическое моделирование технических объектов и систем управления»,
- «Теория игр и исследование операций»,
- «Теоретические основы управления»,
- «Защищённые информационные системы»,
- «Теоретические основы компьютерной безопасности».

Знания, полученные при изучении дисциплины «Концептуальное проектирование информационной безопасности», могут быть использованы при изучении других базовых дисциплин профессионального цикла:

- «Технология обеспечения информационной безопасности объектов»,
- «Управление информационной безопасностью»,
- «Организационно-правовые механизмы обеспечения информационной безопасности».

Структура учебной дисциплины

Область и уровень знаний, цели, которые поставлены при изучении дисциплины, определяют её как базовую дисциплину при подготовке магистров. Обучение на этапе подготовки магистров достаточно насыщено базовыми дисциплинами, поэтому на дисциплину «Концептуальное проектирование информационной безопасности» целесообразно выделить один 2-ой семестр, когда получены необходимые знания по общенаучным циклам и математическому естественнонаучному модулю, но, при этом, предусматривается значительное время на практические занятия и самостоятельную работу обучающихся. Структура учебной дисциплины представлена в табл. 1 и 2.

Таблица 1. Структура трудоёмкости

Семестр	Трудоёмкость., (зач. ед.)	Общий объем курса, (а.ч.)	Лекции, (а.ч.)	Практич. занятия, (а.ч.)	Лаборат. работы, (а.ч.)	СРС, (а.ч.)	Форма(ы) итог. контроля, экз. КР
2	4	144	30	45	0	69	экзамен

В табл. 1 использованы следующие показатели: зачетная единица – 36 академических часов (а. ч.); академический час – 45 минут.

Таблица 2. Структура организации учебного процесса и оценки результатов

№ п.п.	Разделы учебной дисциплины	Недели	Лекции, а.ч.	Практ. зан./ семинары, а.ч.	Лаб. работы, а.ч.	Обязат. текущий контроль (форма*, неделя)	Аттестация раздела (форма*, неделя)	Максимальный балл за раздел **
	2 семестр							
1.	Раздел 1	1-8	15	22		КР8	КИ8	25
2.	Раздел 2	9-15	15	23		КР15	КИ15	25
	Экзамен						Э	50
	Итого за семестр		30	45	0			100

В табл. 2 введены обозначения разделов * – сокращенное наименование формы контроля:

КИ – контроль по итогам;

КР – контрольная работа;

Э – экзамен.

Содержание учебной дисциплины

Содержание дисциплины раскрывается в двух разделах и девяти темах.

Первый раздел «ОСНОВАНИЕ» включает в себя три базовых тематических блока:

- современные сложные кибернетические среды и информационная безопасность;
- база построения СОИБ;
- факторы и предпосылки для концептуального проектирования.

Темы этого раздела связаны с основными понятиями и определениями, характеристикой предметной области сложных кибернетических сред, в интересах которых выполняется концептуальное проектирование ИБ, имеющимися нормативными положениями и сложившейся методологией проектирования СОИБ, обоснованием необходимости концептуального проектирования ИБ. Содержание тем представлено в табл. 3.

Второй раздел «ФАКТОРИЗАЦИЯ» включает в себя также три базовых тематических блока:

- управление жизненным циклом на стадии проектирования;
- архитектурный подход;
- методы анализа и синтеза при концептуальном проектировании.

Темы этого раздела предлагают инструментарий системной инженерии по концептуальному проектированию, раскрывают организационно-методические вопросы при проведении концептуального проектировании ИБ, рассматривают методы и формы представления результатов концептуального проектирования СОИБ. Содержание тем представлено в табл. 4.

Таблица 3. Темы раздела «ОСНОВАНИЕ»

Тема №	Наименование	Содержание
1.	Введение	Предмет концептуального проектирования. Краткое содержание курса. Связь со смежными дисциплинами. Базовые понятия предметной области концептуального проектирования сложных систем и решений. Подходы работы со смыслами при принятии решений в размытых предметных областях.
2.	Сложные кибернетические среды и автоматизированные системы защищённого исполнения	Современные сложные кибернетические среды и информационная безопасность. Автоматизированные информационные системы защищённого исполнения. Понятия информационно-технологического ландшафта, интероперабельности и масштабируемости, катастрофоустойчивости автоматизированных систем. Открытые автоматизированные системы. Централизованная и распределённая обработка информации. Клиент-серверные технологии, сервис-ориентированные архитектуры (SOA). Интеграция ресурсов в рамках ЦОД. «Облачные вычисления» и использование ресурсов по технологиям и регламентам аутсоринга. Новые вызовы информационной безопасности, связанные с тенденциями развития кибернетической среды и информационных технологий.
3.	Нормативные положения по информационной безопасности при проектировании СОИБ	Федеральное законодательство в области ИБ. Постановления Правительства РФ. Указы Президента РФ. Нормативные документы государственных регуляторов в области ИБ. ГОСТы по информационной безопасности (в том числе ИСО/МЭК). Стандарты по криптографической защите. Стандарты информационной безопасности в кредитно-финансовой сфере и при использовании персональных данных.
4.	Методологические подходы к проектированию СОИБ	СОИБ как компонент кибернетической среды и объекта информатизации, системная организация. Субъектно-объектный подход к формированию исходных данных и моделированию состояния информационной безопасности. Модель прогнозируемого нарушителя информационной безопасности. Модели угроз информации, информационных угроз и уязвимостей объекта защиты. Нейтрализация угроз с учётом оценки риска и ущерба при их реализации. Особенности проектирования СОИБ государственных информационных систем. Политика информационной безопасности объекта информатизации и синтез СОИБ. Доверенная среда обработки информации и обеспечение защищённости при проектировании СОИБ в современных условиях.
5.	Факторы и предпосылки для концептуального проектирования СОИБ	Парадигма совмещения жизненных циклов сложных информационных систем и СОИБ. Факторы технической и технологической необходимости концептуального проектирования. Сложность кибернетических сред, современных информационных систем, архитектур построения инфраструктурных систем для обеспечения обработки и передачи информации. Взаимная интеграция информационных процессов и бизнес-процессов. Сущность единой целевой функции для объекта информатизации и объекта защиты. Реализация интероперабельности и масштабируемости в условиях наследования АС, перехода на более эффективные информационные технологии, реорганизации бизнеса и бизнес-процессов. Проблема эффективности построения моделей СОИБ в сложных кибернетических средах с применением традиционных детерминированных методов. Предпосылки для концептуального проектирования ИТ-обеспечения и СОИБ предприятий (организаций), связанные с сущностью их деятельно-

Окончание табл.3

Тема №	Наименование	Содержание
		сти: необходимость решения задач высокой значимости; сложность предмета концептуального проектирования; горизонт планирования в деятельности предприятия (организации); величина и перспективы предприятия (организации) с учётом долгосрочного успешного ведения основной деятельности. Пути совершенствования традиционных подходов к проектированию СОИБ.

Таблица 4. Темы раздела «ФАКТОРИЗАЦИЯ»

Тема №	Наименование	Содержание
6.	Подходы системной инженерии к управлению жизненным циклом на стадии проектирования СОИБ.	Методы управления жизненным циклом в системной инженерии как основа концептуального проектирования. Онтология предметной области СОИБ для информационных систем и объектов информатизации. Системный подход: понятие целевой системы, большая система, сложная система; СОИБ как целевая система, её аспекты – обеспечивающая система и система в операционном окружении; интересы к функционированию и стейкхолдеры. Архитектурный подход: описание целевой системы, представление СОИБ в разных предметных онтологиях окружения, опорный и принципиальный уровни описания СОИБ, интенции и их выражение при концептуальном проектировании СОИБ. Совместное взаимосвязанное и согласованное рассмотрение функций организации (предприятия), среды ее деятельности, функциональных приложений и информационно-коммуникационной инфраструктуры АС и СОИБ.
7.	Методы анализа и синтеза при концептуальном проектировании сложных автоматизированных систем в защищённом исполнении	Целевая функция концептуального проектирования СОИБ. Виды проектов: новая разработка, развитие, модернизация, унификация. Структура проекта, состав компонентов. Выбор вектора эффективности по показателям функциональности, защищённости и совокупной стоимости. Композиционный анализ бизнес-объекта информатизации, автоматизированных систем и их инфраструктуры на платформе информационно-технологического ландшафта. Струк-турно-морфологический анализ объектов и компонентов. Синтез решений по автоматизации/информатизации и СОИБ в целях обеспечения совместимости, интеграции и минимизации совокупной стоимости на опорном и принципиальном уровнях описания архитектурного подхода.
8.	Организационно-методические положения проведения концептуального проектирования	Взаимодействие по тематическим направлениям и координация работ проектирующих групп и специалистов. Выделение, описание и предпроектное обследование объекта защиты. Метод анкетирования: разделы и показатели анкет, способы получения данных, их обработки и формирования исходных данных для проектирования. Инвентаризация информационных ресурсов и защищаемых информационных активов. Определение класса защищаемых АС в соответствии с нормативными актами и методическими документами. Анализ уязвимости кибернетической среды и вложенных средств обеспечения информационной безопасности с учётом класса защищаемых АС и с позиций выбранного вектора эффективности по показателям функциональности, защищённости и совокупной стоимости. Формирование требований к моделям нарушителя и угроз информационной безопасности.

Окончание табл. 4

Тема №	Наименование	Содержание
		Формирование требований к функциональному наполнению и структуризации компонентов СОИБ с учётом вложенных средств кибернетической среды и средств обеспечения доверенного пространства функционирования АС. Синтез структурных компонентов СОИБ, включаемых в архитектуру информационной системы и объекта информатизации.
9.	Представление результатов концептуального проектирования СОИБ	Концептуальное описание моделей нарушителя и угроз, политики информационной безопасности. Модель целевой архитектуры СОИБ как составляющей ИТ-инфраструктуры объекта информатизации (предприятия/организации). Формы представления результатов концептуального проектирования СОИБ, как технической системы: функциональная схема (набор элементов, способ их соединения); принцип действия (взаимосвязь между процессами на различных этапах функционирования средств и компонентов СОИБ); принцип изменения (изменение конструкции, режимов работы и взаимодействия средств и компонентов СОИБ между собой и с окружающей средой); конструктивная схема (определение состава средств и компонентов СОИБ, взаимосвязь между элементами СОИБ и компонентами АС, особенности конструктивного исполнения, оптимальное соотношение параметров). Планы развития СОИБ, согласованные с планами развития бизнес-приложений, ИТ-инфраструктуры и смежных систем. Параметры и модель расчёта совокупной стоимости.

Ожидаемые результаты

Основной ожидаемый результат – формирование платформы необходимых знаний и практических представлений, которые позволят специалистам в области проектирования и эксплуатации систем обеспечения информационной безопасности качественно выполнять проектные работы, а также осмысленно и квалифицированно осуществлять эксплуатацию СОИБ в сложных кибернетических средах. Предполагается, что эти специалисты должны приобрести высокую квалификацию, позволяющую им выполнять функциональные обязанности уровня руководителей проектов, ведущих исполнителей, как при проектировании, так и при эксплуатации СОИБ.

В условиях современного информационного общества изучение данной дисциплины призвано,кроме усвоения конкретных знаний, формировать при подготовке высококвалифицированного специалиста по информационной безопасности такие качества, как строгость в суждениях, творческое и концептуальное мышление, организованность и умение выстраивать процедурную доказательную последовательность, технологическую и системную дисциплинированность, обоснованную ответственность.

СПИСОК ЛИТЕРАТУРЫ:

1. Приказ Министерства образованияи науки Российской Федерацииот 28 октября 2009 г. N 497. ФГОС ВПО по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) «магистр»).
2. Национальный стандарт РФ. ГОСТ РИСО/МЭК15288 – 2005. Информационная технология. СИСТЕМНАЯ ИНЖЕНЕРИЯ. Процессы жизненного цикла систем.
3. ISO/IEC 15288: 2008. Systemsandsoftwareengineering – Systemlifecycleprocesses.

4. Подход системной инженерии к управлению жизненным циклом.Понятийный минимум. Интернет – ресурс.URL: http://techinvestlab.ru/files/495344/se_praxos_1.doc (дата обращения 20.06. 2015).

REFERENCES:

1. Order of the Ministry of education and science of the Russian Federation of 28 October 2009 N 497. FEDERAL STATE INDUSTRY STANDARD of higher professional education in the field of training 090900 «Information security» (qualification (degree) «master»).
2. National standard of the Russian Federation. GOST R ISO/IEC 15288 - 2005. The information technology. SYSTEM ENGINEERING. The life cycle processes systems.
3. ISO/IEC 15288: 2008. Systemsandsoftwareengineering – Systemlifecycleprocesses.
4. The systems engineering approach to lifecycle management. The conceptual minimum. Online resource, http://techinvestlab.ru/files/495344/se_praxos_1.doc