

**Птицына Л. К., Птицын А. В.**

**РАСШИРЕНИЕ ЗНАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ В  
ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММАХ МАГИСТРАТУРЫ**

*Лариса Константиновна Птицына*

*доктор технических наук, профессор*

*ptitsina\_lk@inbox.ru*

*ФГБОУ ВО «Санкт-Петербургский государственный университет*

*телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ),*

*Россия, Санкт-Петербург*

*Алексей Владимирович Птицын*

*кандидат технических наук, доцент*

*pticin@inbox.ru*

*ФГАОУ ВО «Санкт-Петербургский национальный исследовательский*

*университет информационных технологий, механики и оптики»*

*(Университет ИТМО), Россия, г. Санкт-Петербург*

**EXPANSION OF KNOWLEDGE ABOUT INFORMATION PROTECTION  
IN EDUCATIONAL PROGRAMS OF MASTERS**

*Larisa Konstantinovna Ptitsyna*

*Federal State Educational Budget-Financed Institution of Higher Education the*

*Bonch-Bruevich Saint-Petersburg State University of Telecommunications,*

*SPbSUT, Russia, Saint-Petersburg*

*Alexey Vladimirovic Ptitsyn*

*Saint Petersburg National Research University of Information Technologies,*

*Mechanics and Optics (ITMO University), Russia, Saint-Petersburg*

*Аннотация. Представлены условия для развития цифровой экономики, рассмотрены объективные предпосылки для расширения знаний о защите информации в образовательных программах магистратуры, описаны приёмы*

*исследования динамических характеристик квантовых средств криптозащиты, предложены способы сквозной связности квантовых технологий и технологий информационной безопасности.*

***Abstract.** Presents the conditions for the development of the digital economy, considered the objective prerequisites for the expansion of knowledge about information security in graduate education programs, describes the techniques for studying the dynamic characteristics of quantum means of cryptographic protection, proposed ways of end-to-end connectivity of quantum technologies and information security technologies.*

***Ключевые слова:** цифровая экономика, кадры, защита информации, инновации, методология, динамические характеристики.*

***Keywords:** digital economy, cadre, protection of information, innovations, methodology, dynamic characteristics.*

В условиях экономики знаний сфера высоких технологий становится одним из главных поставщиком ключевых решений для перехода к новому технологическому укладу, обеспечивающему инновационное развитие промышленности, бизнеса, образования, экономики и культуры. Наполнение безопасных информационных и телекоммуникационных технологий содержанием, определяемым на основе современных достижений фундаментальной и прикладной науки, является важнейшим этапом совершенствования информационных инфраструктур.

Для эффективного развития рынков и отраслей (сфер деятельности) в цифровой экономике требуется не только высокоразвитая институциональная среда, но и наличие развитых платформ, технологий и инфраструктурной среды.

Ключевые направления создания условий для развития цифровой экономики ассоциируются с кадрами и образованием, формированием исследовательских компетенций и технологических заделов. В подобной ситуации раз-

вitiю содержания образовательных программ магистратуры, связанных с безопасными информационными и телекоммуникационными технологиями, уделяется особое внимание, поскольку к основным инфраструктурным элементам цифровой экономики относится информационная инфраструктура и информационная безопасность.

Появление новых достижений становится иницилирующим фактором для обновления контента учебно-методических комплексов.

В контексте рассматриваемых технологических сочетаний с появлением инновационных разработок средств квантовой криптозащиты проявляется объективная необходимость их интеграции в архитектуру комплексных систем защиты информации и развития методологических аспектов сквозных технологий информационной безопасности.

Предлагаемые расширения учебно-методических комплексов образовательных программ магистратуры, связанных с безопасными информационными и телекоммуникационными технологиями, ориентируются на представление новых знаний об информационно-вычислительных технологиях квантовой криптозащиты.

В систему представления новых знаний включаются:

- определение системы возможных подходов к организации квантовых информационно-вычислительных систем;
- построение моделей процесса квантовой криптозащиты;
- определение динамических характеристик средств квантовой криптозащиты;
- исследование средств квантовой криптозащиты;
- построение моделей комплексных систем защиты информации с квантовыми средствами криптозащиты;
- определение динамических характеристик комплексных систем защиты информации с квантовыми средствами криптозащиты;
- исследование комплексных систем защиты информации с квантовыми средствами криптозащиты.

С позиций защиты информации от несанкционированного доступа средства квантовой криптозащиты, имеющие собственный профиль физических особенностей их реализации [1], рассматриваются в совокупности как одна из подсистем комплексной системы.

В связи с этим раскрывается объективная необходимость формирования новых формализаций, позволяющих, с одной стороны, учесть физические и технологические особенности их реализаций в определении и оценивании типовых профилей качества, а, с другой стороны, обеспечить сквозное связывание с формализациями [2, 3], входящими в методологический профиль оценивания показателей и критериев качества комплексных систем защиты информации от несанкционированного доступа. Указанная необходимость особенно ярко проявляется на этапе сертификации комплексных систем защиты информации от несанкционированного доступа, поскольку при её прохождении требуются объективные доказательства определённой защищённости объекта информатизации в поле возможных угроз.

В систему представления новых знаний вводится описание возможных подходов к разрешению проблемной ситуации, связанной с открытостью вопросов в части определения типовых профилей качества пилотных средств квантовой криптозащиты, показателей и критериев их качества, а также связывания показателей и критериев качества с физическими и технологическими особенностями воплощённых реализаций.

Представляемые подходы распространяются на этап моделирования средств квантовой криптозащиты. На этом этапе жизненного цикла средств квантовой криптозащиты предусматривается два типа формализаций. Первый тип формализаций ориентируется на построение моделей процессов квантовой криптозащиты, а второй тип формализаций — на проведение определения и оценивания показателей качества функционирования исследуемых средств квантовой криптозащиты. При этом принимаются во внимание два аспекта. Первый аспект связан с необходимостью согласования профилей качества

функционирования исследуемых средств квантовой криптозащиты с профилями качества комплексных систем защиты информации от несанкционированного доступа. Второй аспект касается типа исследований, нацеленных на определение и оценивание показателей качества функционирования исследуемых средств квантовой криптозащиты. В представляемых исследованиях прослеживается сквозное связывание предлагаемых решений, касающихся отмеченных аспектов. При сквозном связывании формируется единое математическое обеспечение системы моделирования средств квантовой криптозащиты. При учете особенностей второго аспекта исследований допускается как теоретическая вариативность в формировании исходной информации для моделирования, так и фактологическая вариативность, заполняемая по результатам экспериментальных исследований пилотных реализаций средств квантовой криптозащиты.

Разработка математического обеспечения для моделирования процессов квантовой криптозащиты проводится в контексте объектно-ориентированного подхода к анализу и проектированию информационных систем.

Формирование моделей процессов квантовой криптозащиты базируется на математическом аппарате конечных цепей Маркова. При этом считается, что модели процессов квантовой криптозащиты в дальнейшем смогут использоваться для решения следующих задач:

- составление описаний состояний процессов квантовой криптозащиты;
- определение рационального варианта способов и методов квантовой криптозащиты;
- сравнительный анализ влияния различных способов и методов квантовой криптозащиты на показатели качества их функционирования;
- выбор технологий квантовой криптозащиты.

Рассматриваемый подход к формированию моделей процессов квантовой криптозащиты позволяет отразить многообразие способов, методов и технологических приемов в организации и функционировании возможных вариаций в реализации производимых средств.

Комплексные системы защиты информации с квантовыми средствами криптозащиты моделируются в классе расширенных объектно-ориентированных моделей.

Определение динамических характеристик комплексных систем защиты информации с квантовыми средствами криптозащиты проводится с помощью модифицированных методов свёртки.

В представляемой системе знаний прослеживается сквозная связность динамических характеристик квантовых средств криптозащиты с динамическими характеристиками комплексных систем защиты информации, обеспечивающая подобную связность и на технологическом уровне информационной безопасности информационных инфраструктур.

#### *Список литературы*

1. Квантовая криптография: идеи и практика / под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева. – Минск, 2008. – 392 с.
2. Птицын, А. В. Генерация системно-аналитического ядра безопасных информационных технологий / А. В. Птицын, Л. К. Птицына. – Санкт-Петербург : Издательство Политехнического университета, 2011. – 263 с.
3. Птицын, А. В. Аналитическое моделирование комплексных систем защиты информации / А. В. Птицын, Л. К. Птицына. – Гамбург. Saarbrücken : LAP LAMBERT Academic Publishing, 2012. – 293 с.