УДК 378.147:004.056 **DOI: 10.18413/2518-1092-2025-10-2-0-4**

Прокушев Я.Е.[1]
Заливин А.Н.[2]
Пономаренко С.В.[3]
Пономаренко С.А.[3]

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ УЧЕБНЫХ ПЛАНОВ БАКАЛАВРИАТА И СПЕЦИАЛИТЕТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1)] Российский экономический университет имени Г.В. Плеханова,
Стремянный переулок, 36, г. Москва, 115054, Россия
[2)] Белгородский государственный национальный исследовательский университет,
ул. Победы, 85, г. Белгород, 308015, Россия
[3)] Белгородский университет кооперации, экономики и права,
ул. Садовая, 116а, г. Белгород, 308023, Россия

e-mail: prokye@list.ru, zalivin@bsuedu.ru, kaf-otzi-spec@bukep.ru, www.major@mail.ru

Аннотация
В настоящее время информационные технологии являются одним из важнейших факторов обеспечения стабильного развития России. В этой связи обеспечение информационной безопасности является одним из приоритетных направлений деятельности. Чтобы успешно противостоять угрозам информационной безопасности, необходимо обеспечить подготовку квалифицированных специалистов в данной сфере. Качество их обучения во многом определяется тем, насколько корректно разработана программа подготовки. Анализ публикаций по данной проблематике показал, что подробно рассматривались такие аспекты, как выбор учебных дисциплин, способы и технологии проведения занятий, проводились сравнения состава дисциплин учебных программ из университетов различных стран мира. Однако, по мнению авторов статьи, недостаточное внимание уделялось рассмотрению такой важной проблемы, как определение последовательности изучения преподаваемых дисциплин в рамках создаваемого учебного плана. Данное обстоятельство и обуславливает актуальность тематики статьи. Целью написания данной статьи является разработка комплекса моделей, описывающих не только примерную совокупность дисциплин, но и последовательность их изучения. Результатом выполнения исследований, представленных в статье, является комплекс графических моделей, который демонстрирует примерный состав дисциплин, их преемственность, взаимосвязь и последовательность изучения. Предложенный в работе метод описания взаимосвязи учебных дисциплин может быть использован для анализа уже существующих учебных планов, а также при проектировании новых.

Ключевые слова: подготовка специалистов по информационной безопасности; организация учебного процесса по информационной безопасности; разработка учебных планов

Для цитирования: Прокушев Я.Е., Заливин А.Н., Пономаренко С.В., Пономаренко С.А. Особенности проектирования учебных планов бакалавриата и специалитета по информационной безопасности // Научный результат. Информационные технологии. – Т. 10, № 2, 2025. – С. 38-48. DOI: 10.18413/2518-1092-2025-10-2-0-4

Prokushev Y.E.[1]
Zalivin A.N.[2]
Ponomarenko S.V.[3]
Ponomarenko S.A.[3]

THE FEATURES OF DESIGNING BACHELOR'S AND SPECIALIST'S DEGREE CURRICULA IN INFORMATION SECURITY

[1)] Plekhanov Russian University of Economics,
36 Stremyanny Lane, Moscow, 115054, Russia
[2)] Belgorod State National Research University,
85 Pobedy St., Belgorod, 308015, Russia
[3)] Belgorod University of Cooperation, Economics and Law,
116a Sadovaya St., 308023, Russia

e-mail: prokye@list.ru, zalivin@bsuedu.ru, kaf-otzi-spec@bukep.ru, www.major@mail.ru

Abstract
Currently, information technology is one of the most important factors in ensuring the stable development of Russia. In this regard, ensuring information security is one of the priority areas of activity. In order to successfully counter threats to information security, it is necessary to ensure the training of qualified specialists in this field. The quality of their education is largely determined by how well the training program has been developed. An analysis of publications on this issue showed that aspects such as the choice of academic subjects, methods and technologies of conducting classes were considered in detail, and comparisons were made between the disciplines of curricula from universities around the world. However, according to the authors of the article, insufficient attention was paid to the consideration of such an important problem as determining the sequence of study of the subjects taught within the framework of the created curriculum. This circumstance determines the relevance of the subject of the article. The purpose of writing this article is to develop a set of models that describe not only an approximate set of disciplines, but also the sequence of their study. The result of the research presented in the article is a set of graphical models that demonstrates the approximate composition of disciplines, their continuity, interrelation and sequence of study. The proposed method of describing the interrelationship of academic disciplines can be used to analyze existing curricula, as well as to design new ones.
Keywords: training of information security specialists; organization of the educational process on information security; development of curricula on information security
For citation: Prokushev Ya.E., Zalivin A.N., Ponomarenko S.V., Ponomarenko S.A. The features of designing bachelor's and specialist's degree curricula in information security // Research result. Information technologies. – T. 10, №2, 2025. – P. 38-48. DOI: 10.18413/2518-1092-2025-10-2-0-4

ВВЕДЕНИЕ

Качество подготовки студентов для работы в сфере информационной безопасности зависит от квалификации преподавателей, материального обеспечения учебного процесса, возможности прохождения практических стажировок в организациях.

Однако, еще одним существенным фактором является план обучения студентов. Учебный процесс требуется организовать так, чтобы полученное образование соответствовало ожиданиям как самого студента, так и его будущих работодателей. Учебный план во многом регулирует образовательный процесс, определяет перечень и последовательность преподавания предметов, количество времени, отводимого на их изучение, а также используемые формы проведения занятий. Основное влияние на содержание учебного плана оказывают:

1) требования стандартов в области образования, учитывающих направленность подготовки бакалавров по информационной безопасности (защита компьютерных систем, разработка защищенного программного обеспечения, защита телекоммуникационных систем, аналитическая и правовая деятельность в сфере информационной безопасности и т.п.);

2) требования профессиональных стандартов в сфере обеспечения информационной

безопасности;

3) требования работодателей к квалификационным навыкам сотрудников;

4) тенденции в сфере информационной безопасности, связанные с внедрением новых технологий обмена и обработки информации, появлением ранее неизвестных угроз.

Проблема разработки учебных планов подготовки специалистов в области информационной безопасности актуальна во многих учебных заведениях вне зависимости от места его нахождения. Это подтверждается значительным количеством публикаций на данную тематику учеными из самых разных стран [5, 10, 13, 14]. Концептуальным, методологическим вопросам формирования образовательных программ посвящены работы [4, 12, 16]. В работе [6] исследуются особенности подготовки магистров в области информационной безопасности. Авторами проведен подробный анализ особенностей разработки программ для подготовки магистров в области кибербезопасности. Однако рассматриваемые программы и методы их составления рассчитаны на то, что магистрант уже имеет базовое образование в области информационной безопасности или информационных технологий. В исследовании [19] рассматриваются подходы к разработке программ для подготовки бакалавров в области инженерии безопасного программного обеспечения. В этой работе также приведен набор дисциплин для подготовки специалистов в этом направлении обеспечения информационной безопасности.

В работе [14] рассматриваются принципы, на основе которых выполняется разработка учебных программ по кибербезопасности.

Подробное сравнение подходов к образованию в области информационной безопасности и состава преподаваемых дисциплин в учебных программах, используемых в США и Китае, было проведено в работе [7]. Проблематика стандартизации, сложности перехода к стандартизированным программам обучения в области кибербезопасности в США рассматриваются в работе [8].

В 2017 году в США был разработан отчет «Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity» [11], в котором рабочей группой из представителей разных стран были предложены перечни дисциплин, рекомендуемых для преподавания в области информационной безопасности.

В России достаточно давно действует своя система государственных стандартов в сфере образования [18], также имеются профессиональные стандарты, в которых сформулированы навыки и знания, которыми должны обладать специалисты в области информационной безопасности. Они устанавливают требования к оснащенности учебных заведений, определяют общие принципы организации обучения студентов в зависимости от специальности. При этом образовательные стандарты в России предоставляют университетам достаточно широкие возможности выбора учебных дисциплин.

Исследованию проблематики разработки учебных планов и профессиональных стандартов в области информационной безопасности в России посвящено значительное количество работ Е.Б. Белова, В.П. Лося, А.А. Хорева [1-3] и других ученых.

При рассмотрении работ, затрагивающим различные аспекты организации учебного процесса в сфере информационной безопасности, вопрос формирования последовательности преподавания дисциплин для учебных программ бакалавров и специалистов в области кибербезопасности практически не затрагивался. Не только совокупность изучаемых дисциплин, но и последовательность их рассмотрения во многом влияют на качество учебного плана. Данное обстоятельство обуславливают актуальность и основное направление данной работы. В процессе осуществления исследования требуется ответить на следующие проблемные вопросы:

1) Какова примерная совокупность дисциплин, необходимых для обучения студентов в области компьютерной безопасности?

2) Каков принцип формирования логических связей между изучаемыми дисциплинами?

3) Из каких логически связанных между собой дисциплин состоят отдельные блоки или разделы учебных планов?

4) Какова примерная последовательность изучения дисциплин?

Сформулированные проблемные вопросы обусловили цель работы, которая заключается в разработке моделей, описывающих последовательность изучения дисциплин в рамках учебного плана подготовки бакалавров и специалистов в области компьютерной безопасности. Для достижения поставленной цели работы прежде всего следует определить наиболее эффективные методы исследования предметной области.

Учебный план следует рассматривать как систему, состоящую из взаимосвязанных между собой отдельных элементов – дисциплин. Их корректное объединение в рамках учебного плана должно создать логичную и эффективную систему обучения студентов.

В качестве основных методов при проведении исследования будут использованы подходы, предусмотренные теорией системного анализа. Предметной областью в данном случае является учебный план, который будет декомпозирован на несколько подобластей.

Формирование подобластей плана обучения будет осуществляться на основе основных направлений в обеспечении защиты информации. В данном случае предполагается выполнить условное разделение на следующие направления: компьютерные, организационно-правовые и физические аспекты обеспечения информационной безопасности.

В качестве прикладного средства для анализа взаимодействие элементов учебного плана будет применена методология структурного графического моделирования IDEF3. Особенностью инструментария IDEF3 является наличие логических элементов, позволяющих в явном виде указать условия и последовательность выполнения событий в изучаемой модели. В качестве ограничений рассмотрения предметной области, следует указать, что в данном исследовании рассматриваются вопросы подготовки бакалавров, чьим основным направлением профессиональной деятельности будет обеспечение компьютерной безопасности и администрирование систем защиты информации.

Базовыми принципами, влияющими на состав и последовательность изучения дисциплин в разрабатываемых моделях, являются следующие:

1) Для обеспечения защиты информации при ее обработке с помощью средств вычислительной техники требуются знания принципов работы аппаратных устройств и соответствующего программного обеспечения;

2) Рассмотрение методов защиты информации следует выполнять только после изучения соответствующих способов ее обработки;

3) Для успешной работы требуется знания стандартов и правовых норм, регулирующих деятельность по защите информации;

4) Между дисциплинами A и B имеется взаимосвязь друг с другом, если полученные в результате изучения дисциплины A знания и навыки используются при рассмотрении учебных тем дисциплины B;

5) Необходимо рассмотрение вопросов обеспечения физической защиты объектов защищаемой информационной системы с помощью применения технических средств.

2. Построение графических моделей взаимосвязей учебных дисциплин

На рисунке 1 представлена IDEF3 модель, описывающая примерную последовательность изучения «компьютерных» дисциплин при подготовке бакалавров и специалистов в области кибербезопасности. Рассмотрим подробней особенности модели. На рисунке 1 изображены названия дисциплин и связывающие их логические объекты – перекрестки типа «And». Они подразумевают обязательное завершение изучения всех предыдущих дисциплин перед началом рассмотрения последующих. Перекресток «And/Or», расположенный в правой части диаграммы говорит о том, что для изучения любой из последующих дисциплин (расположены в правом столбце) требуется рассмотрение всех предыдущих (расположены во втором столбце).

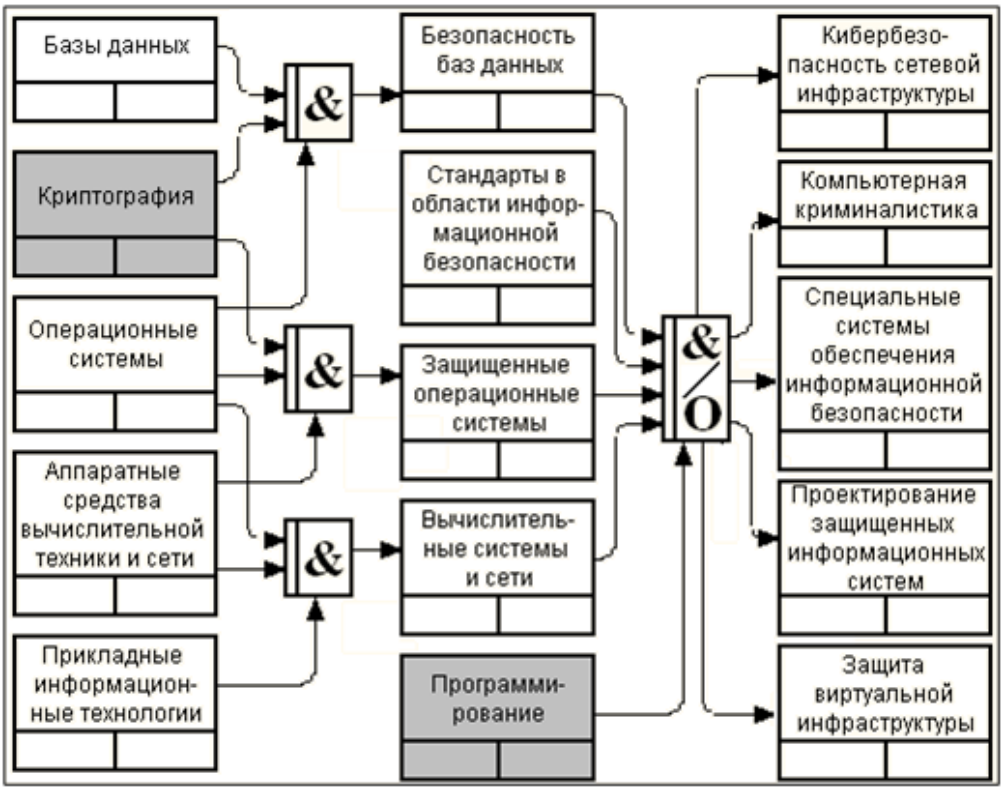

Рис. 1. IDEF3 Модель группы профессиональных дисциплин при обучении бакалавра в области компьютерной безопасности (составлено автором)
Fig. 1. IDEF3 Model of a group of professional disciplines in bachelor's degree studies in computer security (compiled by the author)

Процесс обучения компьютерным дисциплинам можно разделить на несколько этапов. Начальный этап обучения бакалавров в области информационной безопасности должен начинаться с изучения особенностей работы объектов защиты – баз данных, операционных систем, прикладного программного обеспечения, аппаратного обеспечения. На этом же этапе рассматриваются основы криптографии и программирования. Элементы криптографии будут в дальнейшем встречаться во многих дисциплинах, рассматривающих вопросы компьютерной безопасности.

Для рассмотрения вопросов обеспечения безопасности баз данных кроме языка SQL потребуются знание основ криптографии и операционных систем. Используемая операционная система влияет на особенности мер защиты СУБД и обрабатываемых ими баз данных. Также многие СУБД обладают встроенными средствами криптографической защиты хранящихся в них данных. Чтобы применять средства криптографии для защиты баз данных, надо понимать принцип работы криптоалгоритмов и их назначение.

При изучении особенностей защиты сетей потребуются знания в области аппаратных средств вычислительной техники, криптографии и операционных систем.

На третьем этапе подготовки студенты изучают достаточно сложные комплексные дисциплины, требующие предварительной подготовки.

Например, изучение кибербезопасности сетевой инфраструктуры невозможно без предварительного рассмотрения таких дисциплин, как архитектура сетей, операционные систем, безопасность баз данных, стандарты в области информационной безопасности, основы криптографии, аппаратные средства вычислительной техники.

Реализация большого объема высокотехнологичных учебных дисциплин потребует определенного объема финансовых средств. В качестве способа оптимизации финансовых расходов можно предложить использование технологии виртуализации. Применение виртуализации оправдано также тем, что эта технология используются в деятельности самых разных организаций.

Поэтому будущему выпускнику следует ознакомиться с ней, а затем и с особенностями защиты виртуальных объектов.

Относительно таких дисциплин, как Криптография и Программирование следует отметить, что объемы времени, выделяемые на их изучение, могут серьезно отличаться в программах разных учебных заведений. Достаточно часто они образуют отдельные группы взаимосвязанных дисциплин [18]. Для изучения криптографии могут быть предусмотрены дисциплины: основы криптографии, современные криптографические протоколы, криптографическая защита информации и т.п. Программирование может в себя включать курсы, где рассматриваются такие среды программирования, как C++, Python, Java и т.п.

Помимо технических дисциплин большое значение в образовательном процессе играют и гуманитарные. На необходимость изучения гуманитарных дисциплин указано как в работах отечественных ученых [2, 3], так и в зарубежных исследованиях [11].

Например, в документе [11] кибербезопасность определяется как междисциплинарный курс, основанный не только на преподавании технологий обработки и защиты информации, но и изучающий юридические и гуманитарные аспекты обеспечения защиты информации. Эта точка зрения логична по следующим причинам:

1) Преподавание студентам юридических и организационных аспектов мер защиты способно существенно повысить ценность учебной программы, поскольку позволит будущему специалисту системно рассматривать вопросы, связанные с компьютерной безопасностью;

2) В настоящее время большое количество атак начинается не с попыток преодоления существующей системы защиты, а с применения методов социальной инженерии. При этом первым объектом атаки становятся сотрудники организаций.

Точка зрения о необходимости включении гуманитарных дисциплин в учебный план находит свое подтверждение и в работах других авторов [1, 16].

Таким образом, в процессе обучения следует рассматривать психологические, этические, правовые, организационные аспекты обеспечения защиты информации. IDEF3 модель блока правовых и гуманитарных дисциплин показана на рисунке 2.

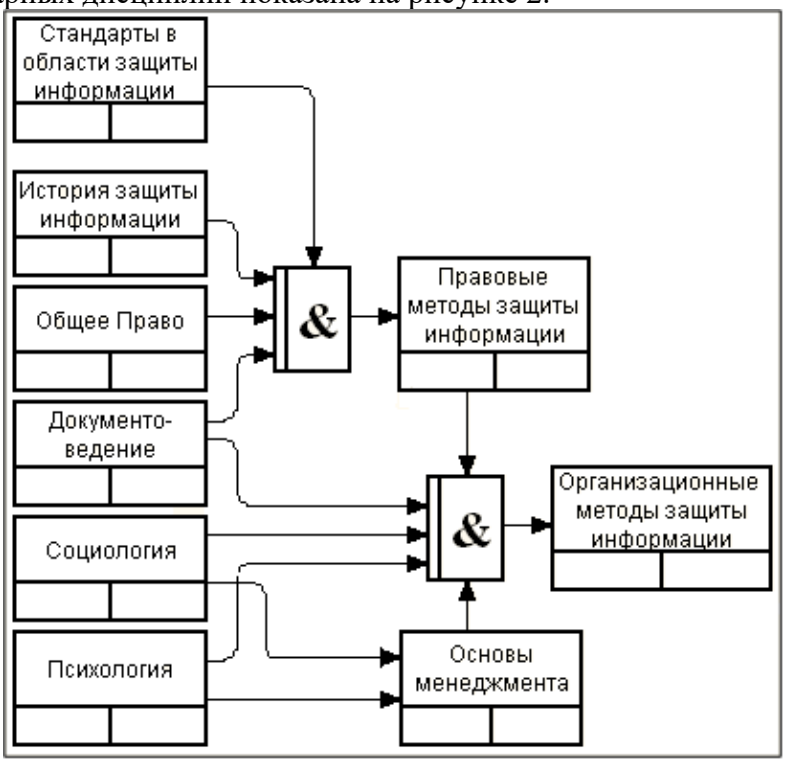

Рис. 2. IDEF3 Модель группы гуманитарных дисциплин при обучении бакалавров в области компьютерной безопасности

Fig. 2. IDEF3 Model of a group of humanities disciplines in Bachelor's degree programs in computer security

Базовую группу гуманитарных дисциплин составляют: социология, психология, документоведение, основы права, история защиты информации, стандарты в области защиты информации, основы менеджмента. Причем основы менеджмента желательно изучать после социологии и психологии. Эти предметы должны рассматриваться с учетом специфики дальнейшей подготовки студентов. Юридические методы, основанные на применении правовых норм в области информационных технологий, играют важную роль в обеспечении компьютерной безопасности. Безусловно, программа подготовки бакалавров в сфере кибербезопасности не должна ставить своей задачей изучение всех тонкостей юриспруденции. Однако нормы законодательства, связанные со своей будущей профессией, бакалавр по компьютерной безопасности знать обязан.

Еще одним важным предметом в данном случае являются методы организационной защиты информации. Эта дисциплина рассматривает меры повышения защиты компьютерных систем с помощью различного рода управленческих решений, норм и регламентов поведения сотрудников на рабочем месте. Изучение этого предмета предполагает предварительное рассмотрение правовых норм, поскольку все внутрифирменные регламенты и инструкции должны соответствовать действующему законодательству.

Методы организационной защиты информации позволяют достаточно эффективно бороться с нарушителями, использующими социальную инженерию. Перед рассмотрением методов организационной защиты следует изучить курсы психологии и социологии.

Рассмотрение технических, организационных и юридических аспектов обеспечения информационной безопасности должно учитывать требования стандартов в области защиты информации (Рисунки 1, 2). Изучение законов, национальных стандартов, ведомственных нормативных документов в сфере информационной безопасности необходимо по следующим причинам:

1) В ряде случаев следование положениям утвержденных стандартов и инструкций может быть необходимо. Их игнорирование может привести к увольнению или даже к судебной ответственности сотрудников, отвечающих за информационную безопасность;

2) В стандартах содержатся готовые подробные методики и инструкции выполнения различных мероприятий в области защиты информации.

Еще одним важным направлением, который следует рассмотреть в процессе обучения студентов, является применение средств обеспечения физической безопасности объектов информатизации: средств осуществления видеонаблюдения, охранной сигнализации, СКУД, систем обеспечения пожарной безопасности. Угрозы техногенных аварий (пожаров), физического уничтожения или хищения носителей актуальны для любой информационной системы. Рассмотрим IDEF3 модель группы дисциплин, обеспечивающих изучение данного аспекта защиты информации (рисунок. 3).

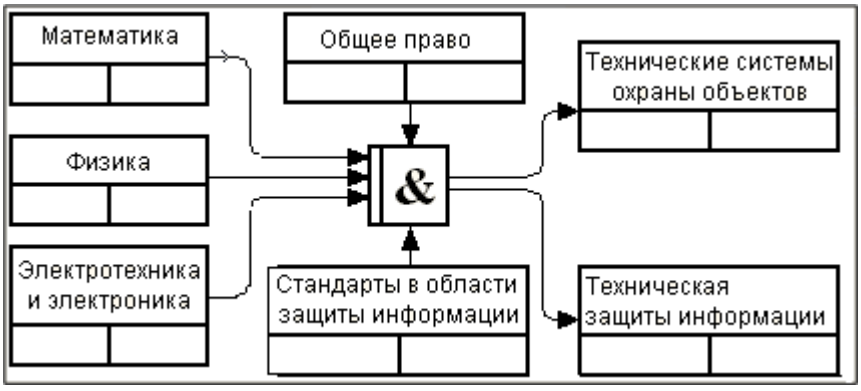

Рис. 3. IDEF3 Модель группы дисциплин при изучении технических средств охраны объектов и технической защиты информации

Fig. 3. IDEF3 Model of a group of disciplines in the study of technical means of object protection and technical information protection

Для изучения систем технической охраны объектов потребуется предварительное изучение таких дисциплин, как математика и физика. Затем следует рассмотреть основы электротехники и электроники. При изучении вопросов внедрения и использования технических систем охраны следует учитывать как технические возможности, так и существующие правовые нормы их применения. Также в данном блоке дисциплин необходимо указать Техническую защиту информации. В рамках данной дисциплины рассматриваются теоретические и практические аспекты работы со специальными техническими средствами, обеспечивающими защиту информации от утечек по техническим каналам.

На завершающем этапе обучения следует предусмотреть дисциплины, где потребуется использовать знания, полученные ранее из разных блоков учебного плана. Например, разработать проект защищенной компьютерной системы (рисунок 4).

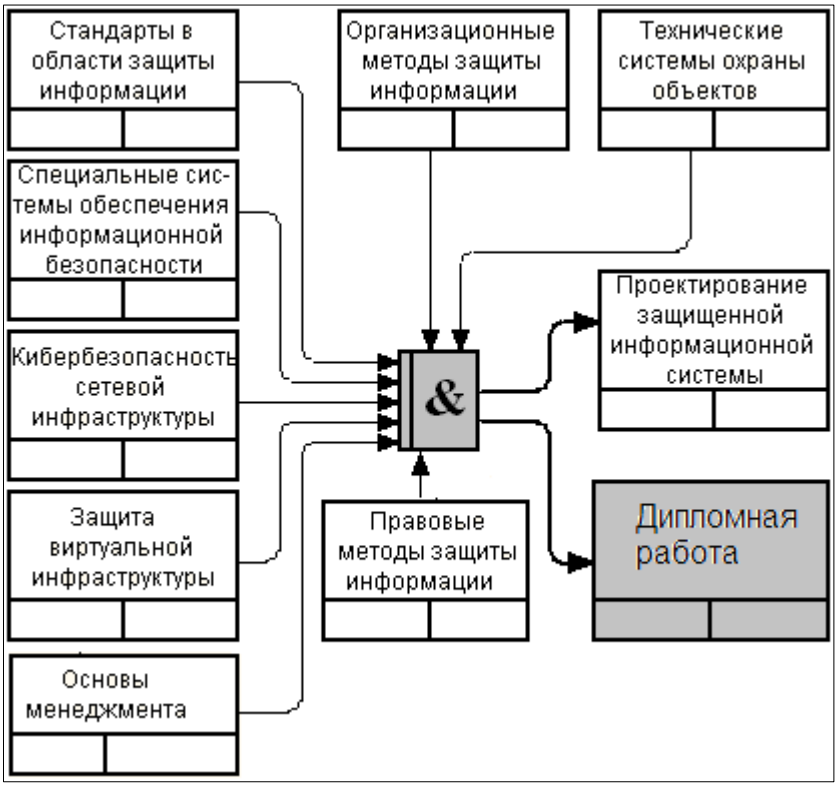

Рис. 4. IDEF3 Модель взаимосвязи базовых дисциплин программы подготовки бакалавров в области кибербезопасности

Fig. 4. IDEF3 Model of the interrelation of the basic disciplines of the Bachelor's degree program in cybersecurity

Дисциплина «Проектирование защищенной информационной системы» позволит объединить полученные ранее знания и навыки в единую взаимосвязанную систему. В рамках ее изучения при выполнении практических заданий студенты должны будут разработать комплекс мер по обеспечению кибербезопасности, применению средств охраны, использованию методов организационной и правовой защиты с учетом особенностей предложенной им для этого организации или ее подразделения.

Завершать курс обучения специалиста в области информационной безопасности должна дипломная (выпускная квалификационная) работа.

3. Выводы и заключение

Представленные в работе модели ориентированы на использование в программах бакалавриата и специалитета по информационной безопасности. При создании программ обучения следует придерживаться целостного, системного подхода, который ориентирован на изучение как технических, так и гуманитарных дисциплин из различных областей научных знаний [9, 15].

Составление учебного плана, основанного на применении только «компьютерных дисциплин», оправдано, если будущий студент уже имеет среднее специальное образование по информационной безопасности или информационным технологиям. В этом случае могут использоваться программы, рассчитанные на обучение в течение трех лет.

Перечень дисциплин, содержащихся в приведенных в этой статье графических моделях, не является шаблоном. Безусловно, названия дисциплин могут отличаться в зависимости от особенностей каждого отдельно взятого университета и направленности программы. Некоторые дисциплины могут быть добавлены в представленные модели. Однако общий принцип формирования последовательности рассмотрения учебного материала должен сохраниться. При построении учебных планов следует сначала рассмотреть общеобразовательные дисциплины, а затем на базе полученных знаний и навыков переходить к изучению специализированных предметов.

В результате проведенных исследований был разработан комплекс графических моделей с использованием нотации IDEF3, описывающих последовательность изучения дисциплин при подготовке бакалавров по информационной безопасности. Модели описывают основные подобласти учебного плана подготовки бакалавров и специалистов по информационной безопасности и рассматривают аспекты обеспечения компьютерной, организационно-правовой и физической безопасности информации. Также разработана модель, которая позволяет синтезировать знания, полученные студентами при изучении дисциплин из отдельных подобластей учебного плана.

Представленные в работе модели разработаны с учетом информационно-логических связей между учебными дисциплинами и содержат рекомендации по последовательности их изучения в рамках программ обучения студентов.

Таким образом заявленная цель исследования, по мнению авторов работы, была достигнута.

Применение графических моделей в процессе создания учебного плана предоставляет возможность оценки корректности установленного порядка изучения дисциплин. В этом заключается практическая ценность предлагаемого метода. Диаграммы, построенные на основе инструментария графического моделирования, наглядно демонстрируют этапы осуществления учебного процесса. Предложенный в статье подход возможно использовать при разработке учебных планов и для других направлений подготовки студентов.

Одним из возможных путей продолжения дальнейших исследований в данном направлении может быть разработка математического аппарата, решающего задачу рациональной расстановки дисциплин.

Список литературы

1. Белов Е.Б., Лось В.П., Зайцева О.М., Кузора И.В. О необходимости актуализации профессиональных стандартов в области информационной безопасности и информационных технологий/ Методы и технические средства обеспечения безопасности информации. – 2020. № 29. с. 119.

2. Белов Е.Б., Хорев А.А. Концептуальный подход к оценке уровней сформированности профессиональных компетенций в области информационной безопасности. Информационное противодействие угрозам терроризма. – 2015. – Т. 2. – № 25. с. 53-62.

3. Белов Е.Б., Лось В.П., Малюк А.А. Цифровая экономика и актуальные проблемы совершенствования системы подготовки кадров в области информационной безопасности. Безопасность информационных технологий, 2018. Т. 25, №. 4. с. 6-22.

4. Asghar M.R., Luxton-Reilly A. Proceedings of the 51st ACM Technical Symposium on Computer Science Education: A Case Study of a Cybersecurity Program: Curriculum Design, Resource Management, and Reflections. Portland, USA. 2020.

5. Bishop M., Miloslavskaya N., Theocharidou M. Proceedings of the 10th World Conference on Information Security Education – WISE10: Information Security Education Across the Curriculum. Rome, Italy. 2015.

6. Cabaj K., Domingos D., Kotulski Z., Respício A. Cybersecurity education: evolution of the discipline and analysis of master programs. Computers & Security, 75(3), 24-35. 2018.

7. Chen H., Maynard S.B., Ahmad A. Proceedings of the 11th Australian Information Security Management

Conference: A comparison of information security curricula in China and the USA. Churchlands, Australia: Edith Cowan University. 2013.

8. Dawson M., Wang P., William K. Proceedings of the 15th International Conference on Information Technology «Information Technology – New Generations»: The Role of CAE-CDE in Cybersecurity Education for Workforce Development. 2018. Vol. 738. Springer.

9. Endicott-Popovsky B.E. Popovsky V.M. Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. ACM Inroads, 2014. Vol. 5, № 1, pp. 57-68.

10. Henry A.P. Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements. Technical Report. ACCS Discussion paper. 2017. Retrieved from https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ ACCS-Discussion-Paper-4-Web.pdf

11. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2018. New York, NY, U.S: Association for Computing Machinery.

12. Kessler G.C., Ramsay J. Paradigms for cybersecurity education in a homeland security program. Journal of Homeland Security Education, 2013. 2, pp. 35-44.

13. Lehto M. Proceedings of the 14th European Conference on Information Warfare and Security: Cyber security competencies – cyber security education and research in Finnish universities. Hatfield, United Kingdom. 2015.

14. Mouheb D., Abbas S., Merabti M. Cybersecurity Curriculum Design: A Survey. Pan Z., Cheok A.D., Mueller W., Transactions on Edutainment XV. Lecture Notes in Computer Science. Berlin, Germany: Springer. 2019. vol 11345. pp. 93-107.

15. Tsado L., Cybersecurity Education: The need for a topdriven, multidisciplinary, school-wide approach. Journal of Cybersecurity Education, Research and Practice, 2019. Vol. 2019. № 1, pp. 37-56.

16. Ward P. Proceedings of the 54th Hawaii International Conference on System Sciences: Constructing a Methodology for Developing a Cybersecurity Program. 2021. pp. 44-53.

17. Yuan X., Yang L., Jones B., Yu H., Chu B. Secure Software Engineering Education: Knowledge Area, Curriculum and Resources. Journal of Cybersecurity Education, Research and Practice, Vol. 2016. No 1, 31-54.

18. Федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность». URL: https://fgosvo.ru/fgosvo/151/150/24/10

References

1. Belov E.B., Los V.P., Zaitseva O.M., Kuzora I.V. On the need to update professional standards in the field of information security and information technology / Methods and technical means of ensuring information security. – 2020. No 29. pp. 119-120.

2. Belov E.B., Horev A.A. A conceptual approach to assessing the levels of formation of professional competencies in the field of information security. Information counteraction to terrorist threats. – 2015. – T. 2. – No 25. pp. 53-62.

3. Belov E.B., Los V.P., Malyuk A.A. The digital economy and actual problems of the improvement of the training system in the field of information security. IT Security (Russia), [S.l.], v. 25, pp. 6-22.

4. Asghar M.R., Luxton-Reilly A. Proceedings of the 51st ACM Technical Symposium on Computer Science Education: A Case Study of a Cybersecurity Program: Curriculum Design, Resource Management, and Reflections. Portland, USA. 2020.

5. Bishop M., Miloslavskaya N., Theocharidou M. Proceedings of the 10th World Conference on Information Security Education – WISE10: Information Security Education Across the Curriculum. Rome, Italy. 2015.

6. Cabaj K., Domingos D., Kotulski Z., Respício A. Cybersecurity education: evolution of the discipline and analysis of master programs. Computers & Security, 75(3), 24-35. 2018.

7. Chen H., Maynard S.B., Ahmad A. Proceedings of the 11th Australian Information Security Management Conference: A comparison of information security curricula in China and the USA. Churchlands, Australia: Edith Cowan University. 2013.

8. Dawson M., Wang P., William K. Proceedings of the 15th International Conference on Information Technology «Information Technology – New Generations»: The Role of CAE-CDE in Cybersecurity Education for Workforce Development. 2018. Vol. 738. Springer.

9. Endicott-Popovsky B.E. Popovsky V.M. Application of pedagogical fundamentals for the holistic

development of cybersecurity professionals. ACM Inroads, 2014. Vol. 5, № 1, pp. 57-68.

10. Henry A.P. Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements. Technical Report. ACCS Discussion paper. 2017. Retrieved from https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/ ACCS-Discussion-Paper-4-Web.pdf

11. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2018. New York, NY, U.S: Association for Computing Machinery.

12. Kessler G.C., Ramsay J. Paradigms for cybersecurity education in a homeland security program. Journal of Homeland Security Education, 2013. 2, pp. 35-44.

13. Lehto M. Proceedings of the 14th European Conference on Information Warfare and Security: Cyber security competencies – cyber security education and research in Finnish universities. Hatfield, United Kingdom. 2015.

14. Mouheb D., Abbas S., Merabti M. Cybersecurity Curriculum Design: A Survey. Pan Z., Cheok A.D., Mueller W., Transactions on Edutainment XV. Lecture Notes in Computer Science. Berlin, Germany: Springer. 2019. vol 11345. pp. 93-107.

15. Tsado L., Cybersecurity Education: The need for a topdriven, multidisciplinary, school-wide approach. Journal of Cybersecurity Education, Research and Practice, 2019. Vol. 2019. № 1, pp. 37-56.

16. Ward P. Proceedings of the 54th Hawaii International Conference on System Sciences: Constructing a Methodology for Developing a Cybersecurity Program. 2021. pp.44-53.

17. Yuan X., Yang L., Jones B., Yu H., Chu B. Secure Software Engineering Education: Knowledge Area, Curriculum and Resources. Journal of Cybersecurity Education, Research and Practice, Vol. 2016. No 1, 31-54.

18. Federal State educational standard of higher education – bachelor's degree in the field of training 10.03.01 "Information security". URL: https://fgosvo.ru/fgosvo/151/150/24/10

Прокушев Ярослав Евгеньевич, кандидат экономических наук, доцент, доцент кафедры прикладной информатики и информационной безопасности, Российский экономический университет имени Г.В. Плеханова, г. Москва, Россия

Заливин Александр Николаевич, кандидат технических наук, доцент, доцент кафедры информационно-телекоммуникационных систем и технологий, Белгородский государственный национальный исследовательский университет, г. Белгород, Россия

Пономаренко Сергей Владимирович, кандидат технических наук, доцент, профессор кафедры информационной безопасности, Белгородский университет кооперации, экономики и права, г. Белгород, Россия

Пономаренко Сергей Анатольевич, доцент кафедры информационной безопасности, Белгородский университет кооперации, экономики и права, г. Белгород, Россия

Prokushev Yaroslav Evgenievich, Candidate of Economics Sciences, Associate Professor, Associate Professor of the Department of Applied Informatics and Information Security, Plekhanov Russian University of Economics, Moscow, Russia

Zalivin Alexander Nikolaevich, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russia

Ponomarenko Sergey Vladimirovich, Candidate of Technical Sciences, Associate Professor, Professor of the Department of Information Security, Belgorod University of Cooperation, Economics and Law, Belgorod, Russia

Ponomarenko Sergey Anatolyevich, Associate Professor of the Department of Information Security, Belgorod University of Cooperation, Economics and Law, Belgorod, Russia