

Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Тамбовский государственный университет имени Г.Р.Державина»

*На правах рукописи*

**Анурьева Мария Сергеевна**

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДГОТОВКИ СПЕЦИАЛИСТОВ  
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
В РОССИИ И ЗА РУБЕЖОМ**

5.8.7. Методология и технология профессионального образования  
(педагогические науки)

Диссертация  
на соискание ученой степени  
кандидата педагогических наук

Научный руководитель:  
Марина Сергеевна Чванова  
доктор педагогических наук, профессор

Тамбов – 2022

## ОГЛАВЛЕНИЕ

Введение.....	3
<b>1 ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ, ВЕЛИКОБРИТАНИИ, США, ГЕРМАНИИ И ФРАНЦИИ .....</b>	
1.1 Научные основы сравнительно-сопоставительного анализа профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах.....	16
1.2 Профессиональное образование будущих специалистов по информационной безопасности в России .....	27
1.3 Профессиональное образование будущих специалистов по информационной безопасности в Великобритании, США, Германии и Франции .....	40
1.4 Анализ отечественного и зарубежного опыта по интеграции образовательных программ с вендорскими образовательными курсами и вендорнезависимой сертификацией.....	67
Выводы по главе 1.....	78
<b>2 СРАВНИТЕЛЬНО-СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ИНТЕГРАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ С ВЕНДОРСКИМ УЧЕБНЫМ КУРСОМ.....</b>	
2.1 Становление системы профессионального образования специалистов по информационной безопасности.....	82
2.2 Общие черты и ключевые различия в компонентах подготовки будущих специалистов по информационной безопасности в России и за рубежом.....	96
2.3 Модернизация содержательной составляющей отечественной системы профессионального образования по информационной безопасности .....	116
2.4 Опытно-экспериментальная работа по интеграции образовательных программ с вендорским учебным курсом.....	129
Выводы по главе 2.....	158
Заключение .....	164
Список использованных источников.....	168
Список иллюстративного материала.....	190
Приложения .....	192

## ВВЕДЕНИЕ

**Актуальность исследования.** В условиях динамичной информатизации обострились проблемы информационной безопасности личности, общества и государства. В последнее десятилетие отмечается скачкообразный рост реализованных угроз в информационной сфере. Объектом постоянного внимания органов государственной власти и общества становятся многочисленные спланированные кибератаки, информационно-психологическое воздействие на индивидуальное и массовое сознание, увеличивающиеся масштабы компьютерной преступности, в том числе сетевое мошенничество и инциденты, связанные с нарушениями прав и свобод граждан при обработке персональных данных.

В Доктрине информационной безопасности Российской Федерации (2016 г.) Правительством обозначены проблемы в информационной сфере, среди которых: отставание отечественных разработок средств защиты информации, слабая осведомленность граждан в вопросах личной информационной безопасности, а также недостаточная кадровая обеспеченность в области информационной безопасности. Профессиональное образование будущих специалистов по информационной безопасности, способных решать соответствующие задачи, является значимым элементом государственной политики, нацеленной на обеспечение защиты интересов в информационной сфере. Изучение опыта зарубежных систем профессионального образования в области информационной безопасности в современных условиях реформирования отечественной системы подготовки специалистов получает свое развитие в контексте государственной потребности.

Все это требует выявления многообразия профессионально-педагогических технологий и лучших практик профессионального образования будущих специалистов по информационной безопасности за рубежом, сравнительного

анализа и обоснования их применения в российской системе при обязательном сохранении уникальности и позитивного отечественного опыта.

**Степень разработанности темы исследования.** В педагогической науке проведены многочисленные исследования по сравнительному анализу отечественного и зарубежного образования. Методологические и теоретические основы компаративистики разрабатывались в трудах Е.В. Андриенко, Б.Л. Вульфсона, А.Н. Джуриного, И.Р. Луговской, З.А. Мальковой, С.Н. Широбокова и др.

Современные исследования, посвященные сравнительно-педагогическому анализу образования и совершенствованию системы профессионального образования специалистов в России проведены, в частности, в работах И.В. Вагиной, О.Н. Зуевой, Э.Э. Исмаилова, Н.В. Кузьменко, А.Ю. Плешаковой, В.С. Пустоцвет и др.

В отечественной педагогике авторами рассматривались отдельные аспекты профессионального образования специалистов по информационной безопасности: Е.В. Белов, А.П. Коваленко, Т.А. Лавина, И.В. Мацкевич, Б.А. Погорелов, И.Д. Рудинский, В.А. Шапошников, В.П. Шерстюк и др. В современных отечественных и зарубежных исследованиях уделяется значительное внимание методическому анализу образовательных программ по информационной безопасности и их интеграции с вендорскими образовательными курсами: С. Аряперума, Р. Браун, А.Дж. Гапински, М. Гроувер, Дж. Кохли, М. Лоттер, Дж. Макводсон, Дж. Мерфи, К. Минхас, А.С. Морозова, Н. Мосс, Б. Рейникл, А. Смит, А.В. Солодянников, В.Н. Соляной и др.

Гуманитарные аспекты информационной безопасности, в том числе проблемы информационной безопасности личности, рассматривались в работах С.Н. Гриняева, В.Н. Лопатина, А.В. Манойло, А.В. Морозова, Е.О. Полушина, В.П. Полякова и др.

Вместе с тем нами не выявлены системные исследования по сравнительно-сопоставительному анализу профессионального образования будущих

специалистов по информационной безопасности в России, США, Великобритании, Франции и Германии.

Таким образом, отечественная система профессиональной подготовки будущих специалистов по информационной безопасности требует сравнительного анализа с зарубежными системами. Анализ научной литературы по педагогическим вопросам подготовки будущих специалистов позволил обосновать проблему исследования, вытекающую из **противоречий** между:

- необходимостью анализа опыта подготовки будущих специалистов в области информационной безопасности в России и зарубежных странах и отсутствием критериев сопоставления для проведения сравнительно-сопоставительного анализа;

- имеющейся спецификой в системах образования специалистов в области информационной безопасности в России и зарубежных странах и дефицитом информации в теории профессионального образования об общих чертах и ключевых различиях между отечественной и зарубежными системами подготовки;

- объективной потребностью современного общества в условиях интенсивной цифровизации в специалистах в области информационной безопасности, способных обеспечить высокий уровень защиты от общемировых угроз в информационной сфере при недостаточной кадровой обеспеченности в области информационной безопасности в России и отсутствием определенных на основе позитивного мирового опыта возможностей модернизации отечественного профессионального образования в области информационной безопасности.

Социальная значимость **проблемы** профессиональной подготовки будущих специалистов по информационной безопасности и фрагментарное несоответствие национальных систем образования специалистов мировым лидерам в данной области определили тему исследования: «**Сравнительный анализ подготовки специалистов в области информационной безопасности в России и за рубежом**».

**Цель исследования:** систематизация сведений и сравнительно-сопоставительный анализ профессионального образования в области информационной безопасности для обоснования рекомендаций по улучшению подготовки специалистов в России.

**Объект исследования:** система профессионального образования будущих специалистов по информационной безопасности.

**Предмет исследования:** сравнительно-сопоставительный анализ профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах (США, Великобритании, Германии и Франции).

**Гипотеза исследования:** применение положительного опыта подготовки специалистов в области информационной безопасности зарубежных стран в отечественной системе профессионального образования обеспечит дополнительную возможность реализации механизмов ее развития и повысит уровень готовности студентов к будущей профессиональной деятельности, если:

- проанализировать в сравнительном плане по сопоставимым критериям подготовку специалистов в области информационной безопасности в России и зарубежных странах;
- сопоставить компоненты системы профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах и обнаружить общие черты и ключевые различия;
- обосновать возможность применения отдельных аспектов позитивного зарубежного опыта, среди которых: интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров.

В соответствии с целью, объектом, предметом и гипотезой исследования были определены следующие **задачи**:

1) Определить критерии сопоставления и провести сравнительно-сопоставительный анализ систем профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах.

2) Выявить общие черты и ключевые различия в компонентах отечественной и зарубежных систем профессионального образования будущих специалистов по информационной безопасности.

3) Выявить и обосновать компоненты модернизации содержательной составляющей отечественной системы профессионального образования по информационной безопасности с учетом позитивного зарубежного опыта и экспериментально проверить влияние изучения вендорского образовательного курса на уровень готовности студентов к будущей профессиональной деятельности.

**Методологическую основу исследования** составили: системный (А.Р. Камалеева, В.А. Слостенин, М.Ю. Федорова, А.П. Шкуратова и др.), информационный (С.И. Архангельский, Л.И. Фишман, Н.О. Яковлева, и др.) и историко-логический (М.С. Чванова и др.) подходы.

**Теоретической основой исследования** являются: исследования компаративистов (Е.В. Андриенко, И.В. Вагина, Б.Л. Вульфсон, А.Н. Джурицкий, О.Н. Зуева, Э.Э. Исмаилов, Н.В. Кузьменко, И.Р. Луговская, З.А. Малькова, А.Ю. Плешакова, В.С. Пустоцвет, С.Н. Ширококов и др.); исследования, связанные с анализом профессиональной подготовки специалистов по информационной безопасности в России и за рубежом (Е.Б. Белов, А.П. Коваленко, Т.А. Лавина, А.А. Малюк, Г.И. Маргаров, И.В. Мацкевич, Б.А. Погорелов, И.Д. Рудинский, В.П. Шерстюк и др.); исследования, касающиеся проблем информационной безопасности личности, общества и государства (В.И. Аверченков, С.Н. Гриняев, В.Н. Лопатин, А.В. Манойло, А.В. Морозов, Е.О. Полушин, В.П. Поляков и др.); исследования, связанные с интеграцией образовательных программ с вендорскими образовательными курсами и вендорнезависимой профессиональной сертификацией специалистов по защите информации (С. Аряперума, Р. Браун, А.Дж. Гапински, М. Гроувер, Дж. Кохли,

М. Лоттер, Дж. Макводсон, Дж. Мерфи, К. Минхас, А.С. Морозова, Н. Мосс, Б. Рейникл, А. Смит, А.В. Солодьянников, В.Н. Соляной).

В качестве **источниковедческой базы** использовались диссертационные исследования по сравнительной педагогике диссертационного зала РГБ, материалы всероссийских и международных конференций по проблемам исследования, материалы научных электронных библиотек Elibrary и Cyberleninka, международных баз научной информации, а также другие электронные источники по теме диссертационного исследования: нормативно-правовая документация в области образования и информационной безопасности, определяющая образовательную политику; материалы, обращенные к проблемам профессионального образования будущих специалистов по информационной безопасности в России и за рубежом; комплекты образовательных программ отечественных и зарубежных вузов: учебные планы, программы дисциплин, практик, итоговых аттестаций, требований к выпускным работам.

Охват зарубежных источников составил около 400 образовательных программ, опубликованных на сайтах образовательных организаций, реализующих профессиональную подготовку будущих специалистов по информационной безопасности. Детально рассмотрено 7 отечественных образовательных стандартов группы направления «Информационная безопасность», а также более 20 зарубежных программ подготовки (Великобритания: Лондонский университет Метрополитен, Стаффордширский университет, Вестминстерский университет и других; США: университет в городе Блумсберг, университет Чаттануга, колледж Мерси и других; Германия: университет прикладных наук в городе Оффенбург, Боннский университет, университет в городе Пассау, университет прикладных наук в городе Бранденбург и других; Франция: Высшая школа Телеком Британ, университет в городе Лимож и других). Выбор зарубежных образовательных программ для детального анализа определялся, прежде всего, полнотой изложения комплектов образовательных материалов (учебных планов, рабочих программ дисциплин, практик, итоговых аттестаций) и их доступностью в официальных источниках.



**Методы исследования.** Для решения задач был применен комплекс теоретических методов исследования (анализ информационных ресурсов сети Интернет, системный анализ информационных источников, описательный, исторический, сравнительно-сопоставительный, метод классификации) и эмпирических методов (анкетирование, тестирование, метод самооценки, статистический).

**Опытно-экспериментальная база исследования:** ФГБОУ ВО «ТГУ имени Г.Р. Державина».

**Основные этапы исследования.**

На первом этапе (2011-2014 гг.) работа включала в себя первичный поиск комплектов образовательных программ по информационной безопасности отечественных и зарубежных вузов; анализ и обобщение материала о системах профессионального образования будущих специалистов по информационной безопасности в России и за рубежом; уточнение методологии исследования; определение критериев сопоставления для проведения сравнительно-сопоставительного анализа; подготовку материалов по результатам исследования к публикации.

На втором этапе (2015-2017 гг.) был проведен анализ источников об историческом развитии и современном состоянии деятельности по защите информации в мире; выполнялся сравнительно-сопоставительный анализ, выявлялись общие черты и ключевые различия; осуществлялась подготовка материалов по результатам исследования к публикации.

На третьем этапе (2018-2021 гг.) выделялись компоненты модернизации содержательной составляющей отечественной системы профессионального образования по информационной безопасности; проводилась опытно-экспериментальная работа; осуществлялась подготовка публикаций; обобщались и систематизировались сведения, формулировались выводы, оформлялась диссертация.

**Научная новизна исследования** заключается в том, что:

– уточнены критерии сопоставления систем подготовки будущих специалистов по информационной безопасности (цель подготовки, направления подготовки и профили, содержание образования, образовательные организации, образовательные технологии, профессорско-преподавательский состав, целевая аудитория, управление содержанием образовательных программ, сложившиеся ступени подготовки), что конкретизирует критериальный аппарат сравнительно-сопоставительных исследований систем профессионального образования в области информационной безопасности;

– впервые получены данные об общих чертах (целевая направленность, многоуровневость образования, требования к подготовке научно-педагогических кадров) и ключевых различиях (в направлениях подготовки и профилях, в содержании, в ступенях подготовки, в управлении содержанием образовательных программ, в образовательных технологиях, в ориентированности студенческих практик и стажировок на бизнес-структуры) компонентов отечественной и зарубежных систем профессионального образования будущих специалистов по информационной безопасности;

– выявлены компоненты модернизации содержательной составляющей отечественной системы профессионального образования будущих специалистов по информационной безопасности и механизмы их реализации, доказана эффективность внедрения в образовательные программы по информационной безопасности вендорского образовательного курса, что отличается от ранее проведенных педагогических исследований обоснованием применения передового позитивного опыта в подготовке специалистов по информационной безопасности зарубежных стран.

**Теоретическая значимость исследования** заключается в том, что:

– применительно к проблематике диссертации эффективно использован системный подход для определения критериев сопоставления систем профессионального образования в области информационной безопасности,

реализация которых может служить основой для проведения сравнительно-сопоставительного анализа по близким направлениям подготовки;

– знание об общих чертах и ключевых различиях систем профессионального образования будущих специалистов по информационной безопасности, об этапах развития отечественной системы профессионального образования специалистов и ее связи с процессом развития информационного общества обогащает теорию профессионального образования;

– уточнен критериально-оценочный аппарат, что дополняет набор средств диагностики уровня готовности студентов старших курсов, обучающихся по образовательным программам блока 10.00.00 «Информационная безопасность», к будущей профессиональной деятельности.

**Практическая значимость исследования** заключается в том, что уточнены компоненты модернизации отечественной системы профессионального образования будущих специалистов по информационной безопасности; разработаны основные образовательные программы по направлениям подготовки 10.03.01 «Информационная безопасность» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», реализуемые ФГБОУ ВО «Тамбовский государственный университет имени Г.Р. Державина», в том числе внедрены дисциплины: «Компьютерная экспертиза», «Расследование компьютерных инцидентов», «Избранные вопросы информационной безопасности»; внедрены вендорские образовательные программы Сетевой академии Cisco в рабочие программы дисциплин «Основы информационной безопасности», «Системы защиты информации в мире»; разработаны электронные учебно-методические пособия.

**Достоверность и обоснованность** результатов исследования достигалась опорой на научно-методологический аппарат, оптимальным сочетанием теоретического анализа и анализа практики вузов мира; применением адекватных предмету методов; преемственностью результатов, полученных на различных

этапах исследования; доказательностью и непротиворечивостью выводов; апробацией результатов, полученных в исследовании.

### **Положения, выносимые на защиту.**

1. В качестве основы для проведения сравнительно-сопоставительного анализа систем профессионального образования будущих специалистов по информационной безопасности целесообразно использовать критерии сопоставления, определенные на основе системного подхода, которые включают: цель подготовки будущих специалистов (как системообразующий фактор), направления подготовки и профили, содержание образования (содержательная подсистема), образовательные организации, образовательные технологии, профессорско-преподавательский состав, целевая аудитория (функциональная подсистема), управление содержанием образовательных программ, сложившиеся ступени подготовки (организационно-управленческая подсистема).

2. Системы профессионального образования будущих специалистов по информационной безопасности в России, США, Великобритании, Германии и Франции имеют общие черты и ключевые различия.

Общими чертами национальных систем профессионального образования будущих специалистов по информационной безопасности являются: цель, которая заключается в формировании у будущих выпускников компетенций, необходимых для квалифицированного решения задач обеспечения информационной безопасности в условиях существования угроз; реализация профессионального образования обеспечивается образовательными организациями среднего, высшего и дополнительного образования; к процессу подготовки привлекаются научно-педагогические кадры, имеющие ученую степень, базовое высшее образование, а также ведущие специалисты со стороны профессионального сообщества.

Ключевые различия между отечественной и зарубежными системами профессионального образования будущих специалистов по информационной безопасности, в первую очередь, выделяются по критериям содержательной

подсистемы (направления подготовки и профили, содержание образования). Основные из них заключаются в следующем.

В большинстве американских, британских, немецких и французских образовательных программах по информационной безопасности отсутствуют дисциплины (модули, темы), связанные с методами технической (инженерно-технической) защиты информации, распространенные в отечественных образовательных программах. Также отсутствуют гуманитарные дисциплины (философия, история и другие), обязательные по отечественным образовательным стандартам или включенные дополнительно образовательными организациями России. Вместе с тем в большинстве зарубежных образовательных программах присутствуют в значительном объеме дисциплины по компьютерной экспертизе и расследованию цифровых преступлений, которые на данный момент не получили широкого распространения в отечественных образовательных программах. За рубежом широко распространены дисциплины экономического блока (менеджмент, управление бизнес-процессами и прочие).

Значительная часть зарубежных образовательных программ по информационной безопасности интегрирована с вендорскими образовательными курсами и содержательно ориентируется на будущую вендорнезависимую сертификацию выпускников.

Ключевые различия, выявленные по критериям функциональной и организационно-управленческой подсистем, не являются специфичными для области профессионального образования будущих специалистов по информационной безопасности и, в большей степени, отражают особенности национальных систем профессионального образования (в ступенях подготовки, в управлении содержанием образовательных программ, в образовательных технологиях, в ориентированности студенческих практик и стажировок на бизнес-структуры).

3. Компоненты модернизации содержательной составляющей отечественного профессионального образования будущих специалистов по информационной безопасности включают:

– переориентацию профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества. Механизмом переориентации может стать включение в образовательные программы дисциплин (модулей), связанных с обеспечением информационной безопасности в бизнес-структурах и расширение сотрудничества образовательных организаций с бизнесом.

– фрагментарное изменение содержания образовательных программ при помощи механизма включения дисциплин по компьютерной экспертизе, расследованию цифровых преступлений и правоприменительным технологиям в сфере защиты информации.

– интеграцию образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров на основе механизма взаимодействия с ИТ-компаниями и включения вендорских образовательных курсов в соответствующие программы дисциплин с возможной итоговой сертификацией.

Включение вендорского образовательного курса с последующей сертификацией в образовательные программы по информационной безопасности обеспечивает повышение уровня готовности студентов к будущей профессиональной деятельности.

**Апробация результатов исследования.** Материалы исследования опубликованы в научных статьях и тезисах, обсуждались на заседаниях кафедры математического моделирования и информационных технологий ТГУ им. Г.Р. Державина и в научных конференциях: Международная научно-практическая конференция «Актуальные проблемы информатики и информационных технологий» (Тамбов, 2011-2017), Всероссийская конференция «Преподавание информационных технологий в РФ» (Саратов, 2011; Воронеж, 2013; Санкт-Петербург, 2016; Москва, 2018), Всероссийская научно-практическая конференция «Информационные технологии в образовании» (Саратов, 2011), Всероссийская научно-практическая конференция

«Державинские чтения» (Тамбов, 2011-2018), Международная научная конференция «Компьютерные науки и информационные технологии» (Саратов, 2016), Международная научно-практическая конференция «Цифровая трансформация образования: отечественный и зарубежный опыт» (Москва, 2021). Основные положения и результаты исследования отражены 22 публикациях, в том числе 8 статей в изданиях, рекомендованных ВАК при Министерстве высшего образования и науки РФ.

**Объем и структура диссертации.** Диссертация состоит из введения, двух глав, заключения, списка использованных источников (204 наименования) и 17 приложений, проиллюстрирована 11 таблицами и 26 рисунками.

# **1 ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ, ВЕЛИКОБРИТАНИИ, США, ГЕРМАНИИ И ФРАНЦИИ**

## **1.1 Научные основы сравнительно-сопоставительного анализа профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах**

Одним из основных принципов государственной политики России в сфере образования в соответствии с Федеральным законом № 273 «Об образовании в РФ» является создание благоприятных условий для интеграции российской системы образования с системами образования других государств на равноправной и взаимовыгодной основе. Мы полагаем, что проведение сравнительных педагогических исследований в современных условиях реформирования отечественной системы профессионального образования специалистов получает свое развитие в контексте государственной потребности.

В рамках нашего исследования будем придерживаться мнения Э.Э. Исмаилова относительно того, что термины «сравнительно-педагогический анализ», «сравнительно-сопоставительный анализ», «сравнительный анализ», «сопоставительный анализ» являются синонимами и носят идентичную смысловую нагрузку [38, с.8].

Первоочередной задачей диссертационного исследования является определение критериев сопоставления и проведение по выделенным критериям сравнительно-сопоставительного анализа национальных систем профессионального образования будущих специалистов по информационной безопасности в России и зарубежных странах.

С целью поиска критериев сопоставления нами будет использован *системный подход* [42, 91, 121]. В работе А.П. Шкуратовой «Методология



системного подхода в педагогике» указывается, в том числе, и на необходимость использования данного подхода в сравнении педагогических систем [119, с.258]. С точки зрения системного подхода важно выявить элементы системы профессиональной подготовки специалистов по информационной безопасности, системообразующие факторы подготовки будущих специалистов, а также выявить критерии сопоставления систем профессионального образования специалистов по информационной безопасности.

Большое значение в проведение сравнительно-сопоставительного исследования отводится *информационному подходу* [18, 19, 107, 120]. С этой точки зрения будем рассматривать, что характеристики объекта и субъекта образовательного процесса изменяются не обособленно под влиянием некоторого потока информации, а под влиянием окружающей среды и иных факторов, которые просто невозможно учесть. Информация же в закрытой управляемой системе не изменяется, она статична. В реальной социальной жизни она динамична и непрерывно совершенствуется [5, с.92].

С точки зрения *информационного подхода* предполагается рассмотрение каждой образовательной программы по информационной безопасности в разных странах как информационной модели. Образовательная программа, реализуемая отечественной или зарубежной образовательной организацией, представляет собой пакет информации, в который, среди прочего, входят сведения о ее структуре, целях, формируемых компетенциях, о содержании дисциплин и практик, о профессорско-преподавательском составе, о технической оснащенности. Весь пакет информации представляет собой информационную модель подготовки будущего специалиста в области информационной безопасности. Задачей применения информационного подхода в рамках нашего исследования является выделение и анализ информационных моделей, необходимых для описания системы профессионального образования специалистов по информационной безопасности и проведения сравнительно-сопоставительного анализа. Вместе с тем, решаемые задачи системного подхода могут послужить основой для исследований при информационном подходе.

Установить причинно-следственные связи процессов формирования системы профессионального образования специалистов по информационной безопасности, проанализировав социально-экономические предпосылки современной системы профессионального образования специалистов рассматриваемого профиля, представляется возможным с использованием *историко-логического подхода* [111; 5, с.92].

С целью определения методики и этапов сравнительного исследования обратимся к анализу научной литературы.

Важным аспектом в сравнительно-педагогических исследованиях является обоснование возможности переноса позитивного зарубежного опыта на отечественную почву. Э.Э. Исмаилов, обобщая мысли зарубежных ученых Р. Хавигхерста, У. Брикмана, И. Кэндла и др., указывает на необходимость учитывать собственную национальную специфику при преемственности зарубежного опыта [38, с.39]. Отечественные компаративисты Б.Л. Вульфсон и З.А. Малькова также обращают внимание на то, что «зарубежный опыт всегда должен «примеряться» к специфическим условиям отечественной системы просвещения» [27, с.43-44].

В соответствии с различными стратегическими документами России по информационной безопасности, подготовка специалистов в данной области является составляющей общей национальной безопасности и, следовательно, перенос зарубежного опыта, без учета специфики рассматриваемой области невозможен. Вместе с тем предполагается поиск возможных компонентов модернизации отечественной системы профессионального образования и механизмов, способствующих совершенствованию в выделенных направлениях.

С целью выделения основных этапов исследования обратимся к подходу И. Кэндла, который выделяет три основных этапа сравнительного исследования образовательных систем, обозначенные в диссертации Э.Э. Исмаилова [38, с.41]:

1. *описательный* (сбор информации об исследуемых системах образования, необходимых для сравнительно-сопоставительного исследования);
2. *историко-функциональный* (выявляются общие и особенные черты,

предпринимаются попытки объяснить полученные результаты, проводя взаимосвязь между социально-экономическими, культурными, политическими факторами и существующей системой образования);

3. *совершенствование образования* (на основе обоснования переноса положительного международного опыта на отечественную почву).

В монографическом исследовании «Теория и методология истории педагогики и сравнительной педагогики» А.Н. Джурицкий также указывает на аналогичную последовательность сравнительно-педагогических исследований: «выделение критериев, оснований, показателей сравнения; сбор информации; вычленение общего (универсального); определение особенного; формулировка рекомендаций» [34, с.51].

На основе анализа исследований, посвященных проблемам сравнительной педагогики (в том числе диссертационных) [24, 33, 36, 46, 83], для достижения поставленной цели и решения необходимых задач был выбран следующий комплекс методов исследования.

*Метод системного анализа информационных источников.* На сегодняшний день в литературе по вопросам профессионального образования специалистов по информационной безопасности накоплен достаточно разнообразный материал. В связи с этим необходимо формирование списка информационных ресурсов, которые станут теоретической базой для проведения сравнительного анализа. В список информационных источников входят учебно-методические материалы, научные статьи, нормативно-правовая документация.

*Метод анализа информационных ресурсов сети Интернет.* Глобальная сеть Интернет – актуальный источник, содержащий последние сведения по заявленной тематике, в которой, благодаря онлайн доступу к ресурсам зарубежных образовательных учреждений, возможно оперативное получение информации по формированию образовательного пространства специалистов по информационной безопасности. Материалы, доступные в сети Интернет, станут основой для выбора оптимальных направлений сравнительно-сопоставительного анализа, и тем самым будут способствовать повышению качества запланированных исследований.

*Описательный метод.* В связи с дефицитом сведений о профессиональном образовании будущих специалистов по информационной безопасности в зарубежных странах применяется описательный метод, задачей которого ставится накопление достаточного объема информации для проведения сравнительно-сопоставительного анализа.

*Исторический метод* предполагает анализ системы профессионального подготовки будущих специалистов по информационной безопасности с учетом влияния исторических факторов на процессы образования.

*Сравнительно-сопоставительный метод* образовательных систем является основным методом нашего исследования, так как позволяет выявить общее и особенное в системах профессионального образования будущих специалистов по защите информации в России и зарубежных странах.

*Метод классификации,* систематизирующий многочисленные образовательные программы в разных странах на основании объединяющего классификационного признака (содержание образовательных программ), позволяет повысить качество проводимого исследования за счет структурирования и систематизации полученной информации.

Для проведения опытно-экспериментальной работы будет применен комплекс *эмпирических методов*, включающий в себя методы анкетирования, тестирования, самооценки, в также статистические методы обработки данных.

Э.Э. Исмаилов отмечает, что цели и задачи сравнительных исследований могут различаться друг с другом и, как следствие, возникает невозможность использования одинакового инструментария сопоставительного анализа [38, с.37]. Соответственно, одной из главных задач нашей диссертационной работы становится разработка основы для проведения сравнительного анализа педагогических систем подготовки будущих специалистов по информационной безопасности при помощи *определения критериев сопоставления.*

В контексте нашего исследования для анализа национальных систем профессионального образования будущих специалистов по информационной безопасности целесообразно выделить следующие критерии для проведения

сравнительно-сопоставительного анализа:

- цель подготовки будущих специалистов по информационной безопасности;
- управление содержанием образовательных программ;
- направления подготовки и профили;
- сложившиеся ступени образования (академические степени);
- образовательные организации;
- образовательные технологии;
- целевая аудитория;
- преподавательский состав, привлекаемый к реализации образовательных программ по информационной безопасности;
- содержание образовательных программ по информационной безопасности [5, с.95].

Н.М. Воскресенская в работе «Некоторые вопросы методологии сравнительной педагогики в Англии в 80-х годах: концепция Б. Холмза», обращает внимание, что важной задачей сравнительно-педагогических исследований английский ученый считает «стремление лучше понять отечественные системы образования... в свете тщательно собранных данных...» [25, с.54]. В статье «Генезис педагогической компаративистики в работах западных исследователей» А.Ю. Плешакова отмечает две основные задачи компаративиста, определенные А.В. Брикманом: сбор корректных данных и проведение интерпретационного анализа этих данных [75, с.69]. В работе «Сравнительная педагогика: актуальные вопросы теории и методологии» Б.Л. Вульфсон отмечает, что существенным элементом сравнительно-педагогического исследования является систематизация новой информации о зарубежных процессах и тенденциях в развитии образования и рассматривает ее как самостоятельную научную задачу [26, с.130]. А также Б.Л. Вульфсон подчеркивает «...плодотворные результаты дают исследования, строящиеся на базе бинарных (парных) сопоставлений...», «...однако при безусловной ценности

бинарных исследований, на их основе нельзя выявить глобальные закономерности развития образования», [26, с.123] – отмечает педагог-компаративист.

Такое утверждение актуально в ключе нашего исследования. В связи с тем, что до настоящего времени не проводились масштабные исследования по сравнительно-сопоставительному анализу организации и содержательного наполнения системы профессионального образования специалистов по информационной безопасности в России и зарубежных странах, нам представляется важным особое внимание уделить описательному этапу и более подробно раскрыть вопросы подготовки будущих специалистов по информационной безопасности в экономически развитых зарубежных странах: США, Великобритании, Германии, Франции.

В отчете по оценке численности специалистов, работающих в сфере информационно-коммуникационных технологий на отечественном рынке труда [39] Ассоциация предприятий компьютерных и информационных технологий РФ отмечает, что в качестве стран-ориентиров, опыт которых по подготовке ИТ-кадров может быть применим в России, рекомендует обращать внимание на опыт следующих экономически развитых государств: США (так как страна является лидером по разработки средств и информационно-коммуникационных технологий); Великобритания и Германия (так как являются лидерами европейской экономики с высокой степенью развития промышленности, но при этом, в отличие от России, не имеют сырьевых ресурсов).

Вместе с тем, в отчете отмечено, что еще в 2009 году общая численность ИТ-специалистов, работавших в российской экономике, составляла 1,47 % от всех работающих или 1,34 % трудоспособного населения, а в США последний показатель таких работников составлял 3,74 %, в Великобритании – 3,16 %, в Германии – 3,14 %. На сегодняшний день общая численность ИКТ-кадров различной квалификации в России составляет около 2,4 % от экономически активного населения, при этом аналогичный показатель в Великобритании – 5 %, во Франции и Германии – по 4 %.

Следовательно, выбранные для рассмотрения страны являются странами-лидерами по подготовке ИТ-кадров и представляют интерес для рассмотрения систем профессионального образования в области защиты информации.

Отдельно отметим, что США исторически опережали СССР в вопросах развития информационных технологий: в этой стране впервые появились компьютерные сети, стали разрабатываться программные и аппаратные платформы и к сегодняшнему дню большинство стран мира (в том числе и Россия) активно используют зарубежные информационные продукты.

Правительство Великобритании начало заниматься проблемами защиты информации раньше остальных европейских государств [47, с.53], а Германия традиционно является одной из ведущих держав мира в индустриально-технологическом отношении, где киберзащита критической инфраструктуры в современных условиях является одной из ключевых задач политики национальной безопасности государства [21, с.10].

Франция в настоящее время также является ключевой страной на мировой арене в вопросах безопасности в киберпространстве. В 2018 г. президент Франции обратился к общественности с декларацией под названием «Парижский призыв к доверию и безопасности в киберпространстве» [149]. Эта декларация затрагивала вопросы по выработке общих принципов обеспечения безопасности в киберпространстве и получила поддержку со стороны других государств, частных компаний и общественных организаций. «Парижский призыв» свидетельствует об активной роли Франции в создании безопасного киберпространства.

В США, Великобритании, Германии и Франции уделяется значительное внимание вопросам защиты информации и профессиональной подготовке специалистов и, как отмечалось в отчете Ассоциации предприятий компьютерных и информационных технологий РФ, опыт этих стран может быть полезен для нашей страны.

К настоящему времени в России сформирована специфическая система профессионального образования специалистов по информационной безопасности, базирующаяся на «ментальной закрытости». Требования организаций-

работодателей к выпускникам постоянно ужесточаются и изменяются. Отечественная система подготовки, в большей степени, ориентируется на защиту конфиденциальности информации, в том числе государственной тайны. Однако на сегодняшний момент бóльший процент работодателей для выпускников по специальностям информационной безопасности – это работодатели частного сектора. Это связано с повсеместной информатизацией бизнеса. Постепенно акцент защиты информации с сохранения конфиденциальности различных тайн переносится на сохранение целостности, доступности и конфиденциальности информации в частном секторе, что диктует несколько иное содержание профессионального образования специалистов по информационной безопасности.

Следует отметить, что в связи со спецификой деятельности, как отечественных, так и зарубежных, специалистов по защите информации, их подготовка ведется как в «гражданских», так и в ведомственных вузах, организованных при различных специальных службах. Объектом нашего исследования будут образовательные программы только «гражданских» вузов, в связи с тем, что ведомственные образовательные организации предполагают полную «закрытость» программ обучения.

Для уточнения понятия «специалист в области информационной безопасности» вначале обратимся к словарям, определяющим термин «специалист». Толковый словарь Д.Н. Ушакова [96] дает следующее определение «специалист – это представитель той или иной специальности (научной, художественной, технической и т. п.), человек, профессионально занимающийся тем или иным видом специального труда». Другое толкование: «специалист – работник получивший подготовку к избранному им виду трудовой деятельности в профессиональном учебном заведении» [84].

В соответствии с Единым квалификационным справочником должностей руководителей, специалистов и служащих занимать должность *специалиста в области информационной безопасности* может сотрудник, имеющий высшее образование по специальности «Информационная безопасность» (за исключением должности «техник по технической защите информации» для которой достаточно



среднего профессионального образования по информационной безопасности). В настоящее время к таким специальностям относят все образовательные программы группы 10.00.00 «Информационная безопасность», где к уровню высшего образования относятся программы бакалавриата, специалитета и магистратуры.

К аналогичному выводу приводит изучение группы профессиональных стандартов «Специалист по информационной безопасности»: специалистом по информационной безопасности, в соответствии с данными документами, может быть работник, имеющий высшее образование (бакалавриат, специалитет, магистратура) в данной области.

Соответственно, в диссертационном исследовании под понятием «специалист в области информационной безопасности» будем понимать выпускников, окончивших обучение по образовательным программам бакалавриата, магистратуры или специалитета по соответствующим направлениям подготовки и специальностям. Вместе с тем будем считать, что понятия «специалист по защите информации», «специалист по информационной безопасности», «специалист в области информационной безопасности» носят идентичную смысловую нагрузку.

Таким образом, в параграфе:

- показано, что для проведения сравнительно-сопоставительного анализа систем профессионального образования будущих специалистов по информационной безопасности целесообразно применение методологических подходов: системного, информационного и историко-логического;
- уточнены этапы сравнительно-педагогического анализа;
- выбраны методы исследования, в том числе теоретические: анализ информационных ресурсов сети Интернет, системный анализ информационных источников, описательный метод, исторический метод, сравнительно-сопоставительный метод, метод классификации и эмпирические: анкетирование, тестирование, метод самооценки, статистический.

– обозначены критерии сопоставления для анализа систем профессионального образования будущих специалистов по информационной безопасности;

– обоснован выбор стран для проведения сравнительно-сопоставительного исследования. В связи с тем, что до настоящего времени не проводились исследования о содержании и организации подготовки кадров в сфере информационной безопасности в России и ведущих зарубежных странах, сделан вывод о необходимости более подробного изучения объекта в США, Великобритании, Германии и Франции (которые являются странами-лидерами по подготовке ИТ-кадров и представляют интерес для рассмотрения систем профессионального образования специалистов по защите информации).

## **1.2 Профессиональное образование будущих специалистов по информационной безопасности в России**

Отечественная система образования в области защиты информации начала формироваться в 90-х гг. XX века. Главной причиной тому послужило начало масштабной информатизации общества: постепенно во все сферы стали проникать информационные технологии и, как следствие, угрозы информационно-коммуникационного характера стали получать все большее распространение. Вместе с тем отдельные элементы системы появились еще до XX века и заключались, прежде всего, в изучении математических основ защиты информации в рамках обучения специалистов специальных служб. Несколько позже, с появлением технических средств передачи информации, сотрудников спецслужб стали обучать защите информации от утечки по техническим каналам информации. Но сама система подготовки в современном виде начала получать свое развитие несколько десятилетий назад, в 90-е годы прошлого столетия [16, с.111-112].

На сегодняшний день отечественная система образования в области защиты информации реализуется в системе высшего и среднего профессионального образования, формируется и контролируется через реализацию нормативно-правовых актов в сфере образования при участии государственных и общественных структур (рисунок 1, стр.29) [16, с. 112; 77].

В монографии «Аспекты информационной безопасности в информационной подготовке» В.П. Поляков отмечает, что «для ряда министерств и ведомств (в первую очередь силовых) сформированы ведомственные подсистемы подготовки кадров» [79, с.47]. В рамках такой подготовки реализуются образовательные программы конфиденциального характера, не подлежащие открытому опубликованию. Как уже отмечалось выше, в нашем исследовании будут рассматриваться образовательные программы только «гражданских» вузов, в связи с тем, что ведомственные образовательные организации предполагают

полную «закрытость» программ обучения.

Кроме того, в отечественной системе профессионального образования будущих специалистов по информационной безопасности получило широкое распространение дополнительная профессиональная переподготовка, которая включает в себя курсы повышения квалификации. Как правило, содержание курсов повышения квалификации формируется под запросы потребительского рынка, при этом все программы курсов переподготовки по информационной безопасности должны быть составлены на основе разработанной соответствующими органами (в сфере их компетенций) примерных образовательных программ и согласовываться с ними [81].

В профессиональных стандартах по группе занятий (профессий) «Специалисты в области информационной безопасности» (рисунок 1) отражены квалификационные требования специалистов. Нужно отметить, что кроме пяти, представленных на рисунке 1 профессиональных стандартов, аналогично образовательным программам, имеются профессиональные стандарты для «закрытого» использования при выполнении служебных обязанностей, а также для формирования образовательных программ по «закрытым» специальностям в ведомственных образовательных организациях.

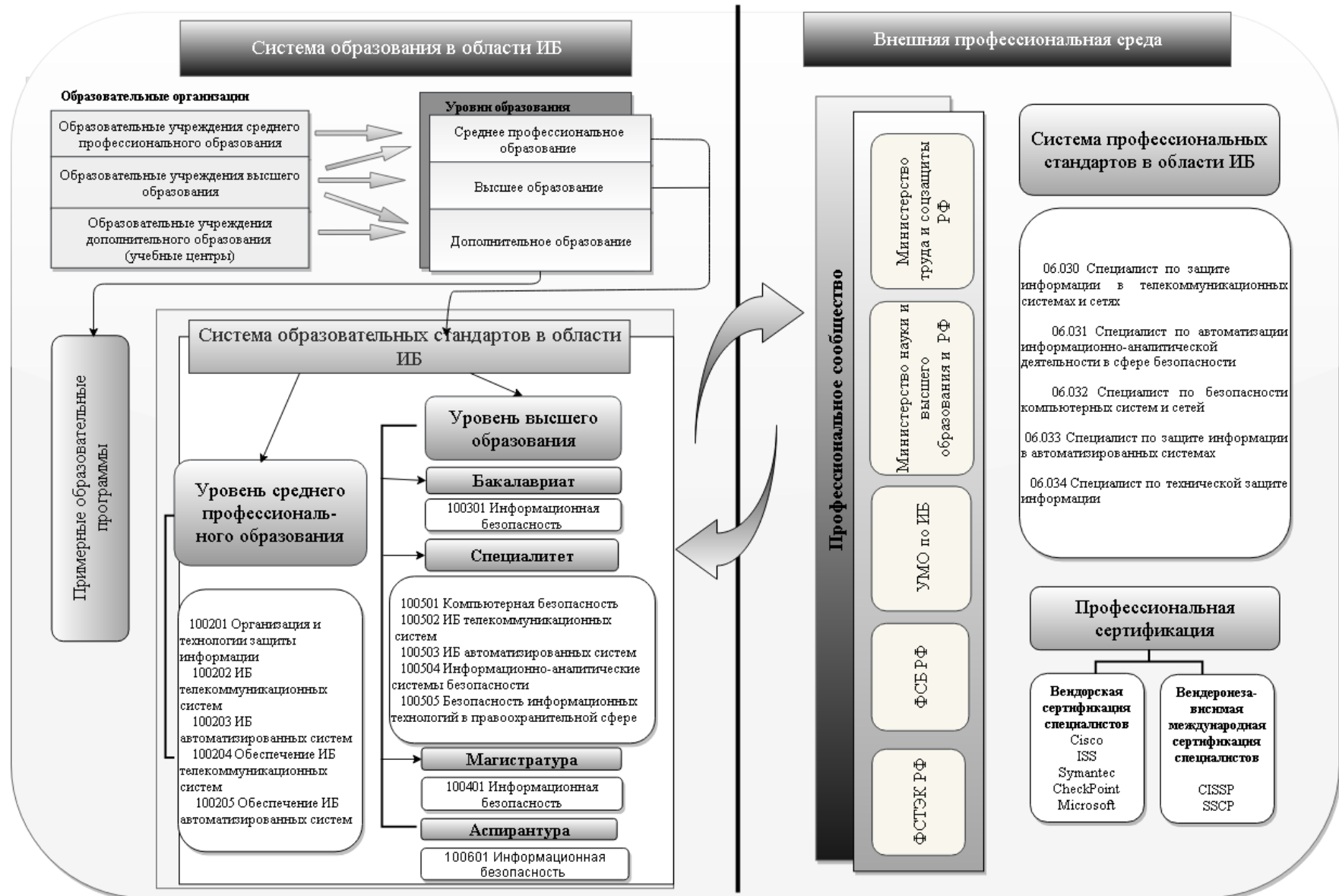


Рисунок 1 – Отечественная система образования в области ИБ и ее взаимосвязь со сферой профессиональной деятельности.

На сегодняшний день отечественная система подготовки по защите информации представлена на всех имеющихся уровнях образования в России. До 2011 года в России, в основном, реализовывались образовательные программы с присвоением квалификации «специалист» (рисунок 2), образовательные программы бакалавриата и магистратуры практически не встречались в нашей стране.

В 2011 году все отечественные вузы начали массово переходить на двухуровневую систему подготовки, что также коснулось и сферы профессиональной подготовки по информационной безопасности.

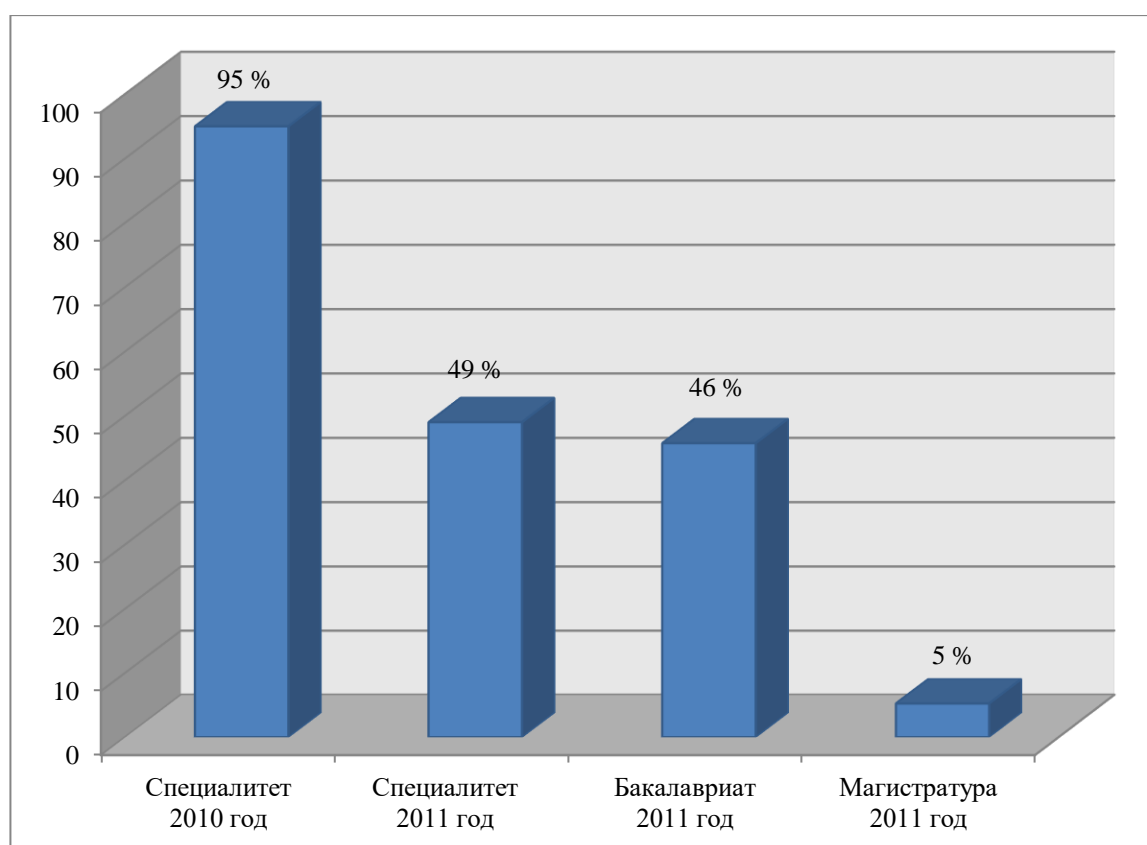


Рисунок 2 –Количество реализовавшихся образовательных программ по уровням подготовки в 2010 и 2011 годах.

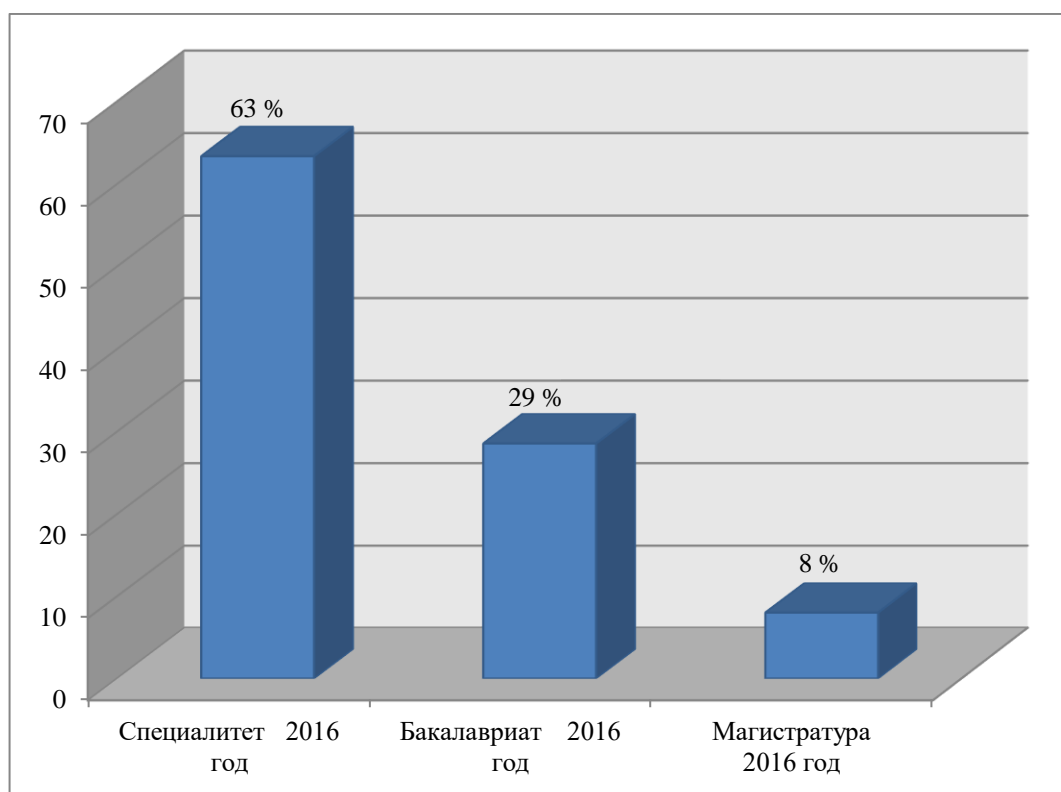


Рисунок 3 – Количество реализовавшихся образовательных программ по уровням подготовки в 2016 году.

Из рисунка 2 видно, что до 2011 года только 5 % образовательных программ по информационной безопасности имели уровень бакалавриата и магистратуры, а остальные 95 % – реализовывали программы специалитета по разным специальностям. В первый год масштабного перехода на двухуровневую систему подготовки в России половина вузов перешли на двухуровневую систему. Спустя пять лет, в 2016 году (рисунок 3), доля специалитетов увеличилась более чем на 10 %, что говорит о востребованности данного уровня подготовки на отечественном рынке труда [16, с. 116].

Современная тенденция к взаимодействию высшего образования с профессиональным сообществом, безусловно, отражается и на профессиональном образовании специалистов по защите информации и, среди прочего, проявляется в том, что ФГОС ВО ориентируют на использование профессиональных стандартов при формировании конкретной образовательной программы, реализуемой в образовательной организации.

В ноябре 2020 года были утверждены приказами Министерства науки и высшего образования РФ (в феврале 2021 года зарегистрированы Министерством юстиции РФ) новые ФГОС ВО [97-103]. В соответствии с данными приказами, прием на обучение по образовательным программам по стандартам, утвержденным в 2016 году, прекращается 1 марта 2021 года.

ФГОС ВО по УГСНП 10.00.00 «Информационная безопасность», утвержденные в ноябре 2020 года представляют собой стандарты поколения 3++ и ориентируются на соответствующие профессиональные стандарты [82] (рисунок 4).

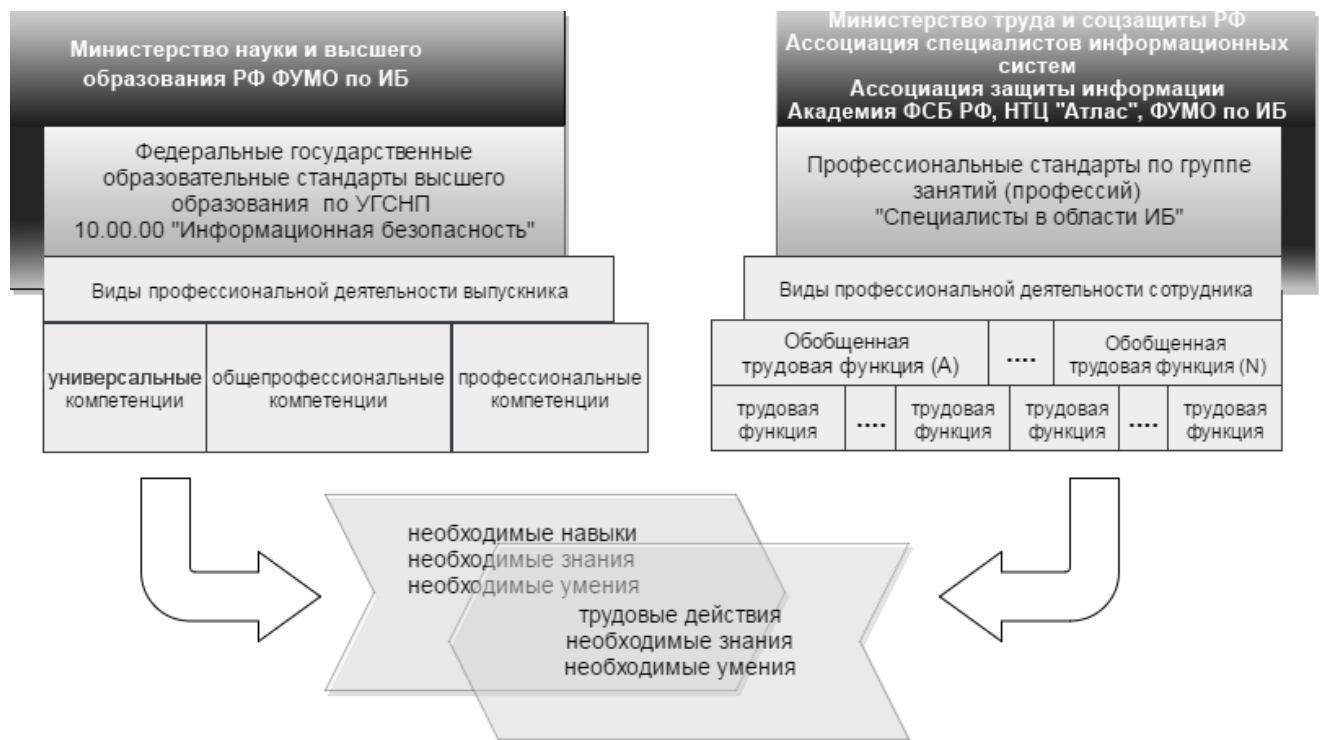


Рисунок 4 – Интеграция профессиональных стандартов по информационной безопасности и образовательных стандартов.

Одним из отличий от стандартов предыдущего поколения стало изменение областей профессиональной деятельности выпускников. В основном к ним относятся области: 01 «Образование и наука (в сфере научных исследований)», 06 «Связь, информационные и коммуникационные технологии (в сфере конкретного направления подготовки или специальности)» и 12 «Обеспечение безопасности (в



сфере конкретного направления подготовки или специальности)». Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» готовит выпускников только к одной области профессиональной деятельности – 12 «Обеспечение безопасности (в сфере защиты информации)», а специальность 10.05.04 «Информационно-аналитические системы безопасности» помимо трех вышеперечисленных областей, дополнительно охватывает область – 08 «Финансы и экономика (в сфере финансового мониторинга в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма)».

В типах задач профессиональной деятельности, к решению которых готовятся выпускники в рамках освоения программ бакалавриата, специалитетов и магистратуры существенные изменения (по сравнению со стандартами предыдущего поколения) нами не были обнаружены.

Следующим значительным отличием новых стандартов от стандартов предыдущего поколения является отсутствие списка профессиональных компетенций непосредственно в образовательном стандарте. Изменился список обязательных дисциплин для включения в образовательные программы. Однако проведение анализа новых обязательных дисциплин вне контекста конкретных образовательных программ будет малоинформативным и нами проводиться не будет.

Следует отметить, что существенной отличительной чертой ФГОС ВО последних поколений по всем принятым в РФ направлениям подготовки является практически полное отсутствие обязательных дисциплин, что было характерно для всех образовательных стандартов, действующих ранее. Однако для направлений подготовки по информационной безопасности современные стандарты обязуют образовательные организации включать расширенный список обязательных для включения в учебные планы дисциплин, обеспечивающий комплексный подход к защите информации.

### 1.2.1 Образовательные программы в области информационной безопасности в РФ

На сегодняшний день уровень среднего профессионального образования (СПО) в области информационной безопасности представлен набором из пяти специальностей (рисунок 1, стр.29), образовательные программы на основе них могут реализовывать отечественные колледжи и вузы. Образовательные программы СПО завершаются присвоением квалификации *техник по защите информации*. Как отмечают авторы, «выпускник организации СПО по направлениям подготовки, связанным с информационной безопасностью, занимает особое место на рынке труда...» так как могут занимать должность техника по защите информации [73, с.40].

В рамках нашего исследования будем проводить обзор программ высшего образования, к которым относятся образовательные программы бакалавриата, магистратуры и специалитета. Вместе с тем, учитывая безусловную важность среднего профессионального образования в данной области, полагаем, что сравнительно-сопоставительный анализ таких программ, а также программ аспирантуры может стать предметом отдельных исследований в сравнительной педагогике.

Рассмотрим образовательные программы, реализуемые в последние 10 лет в образовательных организациях в РФ. На рисунке 5 показано количественное распределение образовательных программ в области информационной безопасности по направлениям подготовки и специальностям.

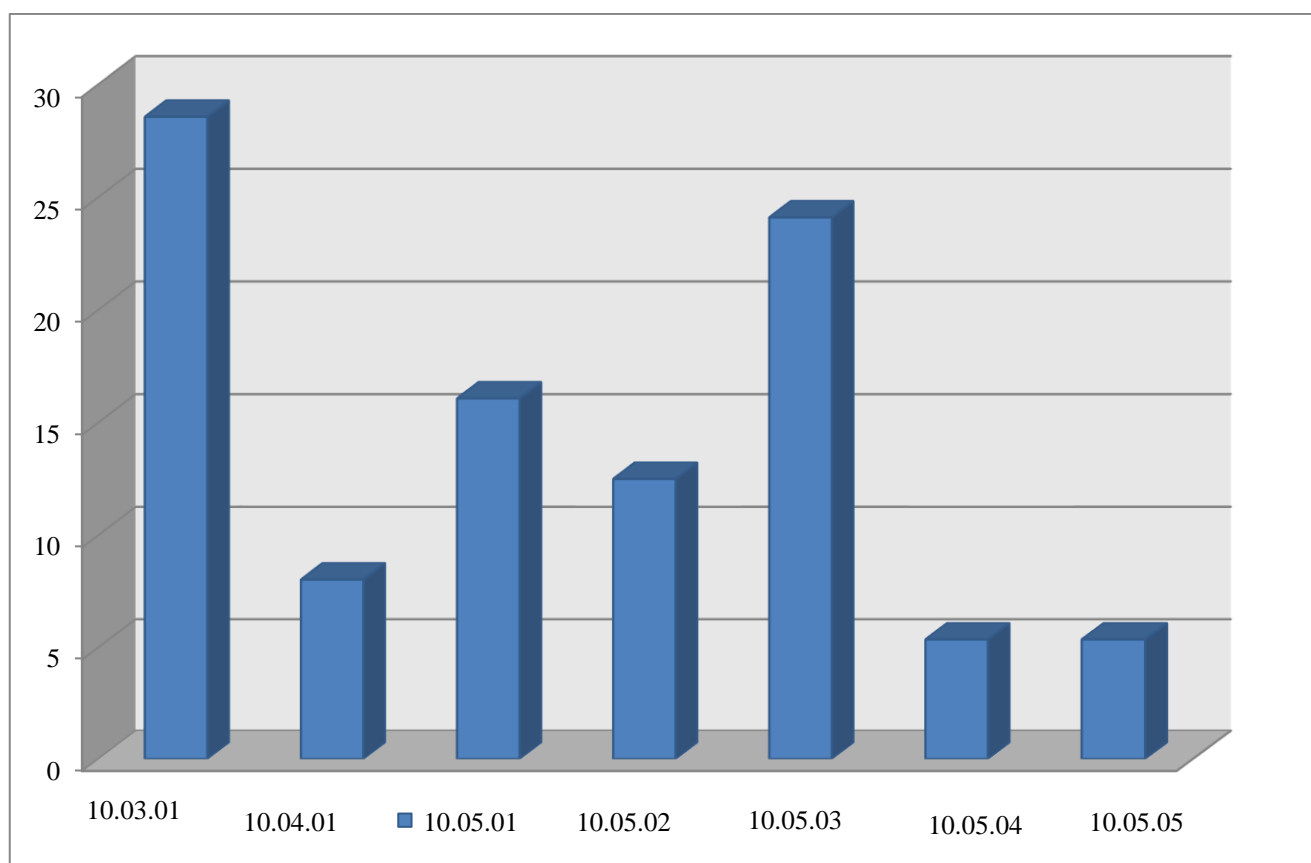


Рисунок 5 – Количество программ бакалавриата, специалитета и магистратуры по направлениям подготовки и специальностям (2016 год).

Из рисунка 5 видно, что 29 % от числа всех образовательных программ по информационной безопасности приходится на программы бакалавриата. Программы магистратуры составляют лишь 8 % от всех программ по информационной безопасности, на программы специалитета по всем направлениям приходится, как сказано выше, большая часть – 63 % [7, с.13-14].

Среди специалитетов самыми популярными образовательными программами в России являются программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем» (24% от всех рассмотренных программ). Более детальное рассмотрение образовательных организаций, ведущих подготовку по данному направлению, показывает, что это, в абсолютном большинстве, технические университеты. Именно технические вузы исторически первыми начали готовить студентов по специальностям, связанным с защитой информации. Таким образом, специфика технического

образования, популярность образовательных программ по автоматизации различных областей хозяйственной деятельности обусловили необходимость защиты таких систем автоматизированного проектирования и введения соответствующих образовательных программ [7, с.14].

Следующие по популярности – образовательные программы по специальностям 10.05.01 «Компьютерная безопасность» (16 %) и 10.05.02 «Информационная безопасность телекоммуникационных систем» (13 %), эти программы направлены на обеспечение безопасности данных в компьютерных системах и сетях.

Менее популярными являются относительно новые специальности: 10.05.04 «Информационно-аналитические системы безопасности» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», на каждую приходится по 5% от числа всех рассмотренных программ.

Рассмотрение обязательных дисциплин, регламентируемых ФГОС ВО, и дисциплин, включенных в учебные планы конкретных образовательных организациях ВО, которые осуществляют подготовку по программам в области информационной безопасности, показывает, что все образовательные программы бакалавров, специалистов и магистров обеспечивают комплексное обеспечение информационной безопасности за счет включения расширенного списка обязательных дисциплин. В то же время в программах специалитетов рассматриваются специфичные вопросы конкретной области профессиональной деятельности.

Детальное рассмотрение дисциплин, входящих в реализуемые на данный момент отечественные образовательные программы, позволяет сделать следующие выводы:

1. Перечень обязательных для изучения профессиональных дисциплин в соответствии со ФГОС ВО включены во все рассмотренные образовательные программы по информационной безопасности.

2. Зачастую при формировании новых образовательных программ частично сохраняются дисциплины, являющиеся обязательными для ранее

действующих образовательных стандартов, что обеспечивает прочную основу для дальнейшего изучения как естественно-научного, так и технического блока обеспечения информационной безопасности.

Содержательный анализ образовательных программ по информационной безопасности представлен в работах авторов (Е.Б. Белов, Л.А. Ильина, А.П. Коваленко, Т.А. Лавина, И.В. Мацкевич, Д.Я. Околот, Б.А. Погорелов, И.Д. Рудинский) [23, 44, 50, 76, 85].

С целью формулирования ориентированности предметной области образовательных программ обратимся к утверждению Е.Б. Белова о том, что «основными объектами информационного воздействия являются: *информационно-технические системы* и средства различного назначения, *информативные признаки объектов, защищаемых от противоправных посягательств*, а также *личность, общество, государство*» [23, с.32-33].

Таким образом, применительно к предметной области образовательных программ по информационной безопасности в России можно выделить следующие составляющие:

– *естественно-научная составляющая информационной безопасности* (сюда относятся специальные разделы математики, криптографическая защита информации, программирование, методы программно-аппаратной защиты информации и т.д.);

– *техническая составляющая информационной безопасности* (противодействие техническим разведкам, инженерно-технические методы защиты информации и т.д.);

– *гуманитарная составляющая информационной безопасности* (борьба с компьютерными преступлениями, защита от психологического воздействия на личность, организационная, правовая и страховая защита информации).

Анализ образовательных стандартов и реализуемых в соответствии с ними образовательных программ позволяет сформулировать следующие выводы:

– большинство отечественных образовательных программ по информационной безопасности ориентируется, в большей степени, на

техническую и естественно-научную составляющие. Акцент на техническую сторону, на наш взгляд, обусловлен аспектами исторического развития государственной системы защиты информации. Естественно-научная составляющая обеспечивается изучением программно-аппаратных методов защиты информации, базирующихся на математических основах обеспечения информационной безопасности, алгоритмизации и программировании;

– отечественные образовательные программы по информационной безопасности также ориентированы на изучение вопросов *правовой стороны гуманитарной составляющей* информационной безопасности. Мы полагаем, что это обусловлено тем, что национальная безопасность страны в целом, информационная безопасность в частности, базируется на нормативно-правовых документах России. Вместе с тем, незначительная содержательная часть образовательных программ по информационной безопасности посвящена иным проблемам гуманитарной составляющей: расследованию цифровых инцидентов, обеспечению информационно-психологической безопасности граждан и общества;

– профессиональное образование будущих специалистов по информационной безопасности формирует способности решать задачи обеспечения безопасности данных в государственных организациях и организациях иных форм собственности. Однако основной акцент делается на деятельность по защите информации в строгом соответствии с государственными регуляторами;

– к положительным сторонам российского профессионального образования будущих специалистов по информационной безопасности можно отнести базовую естественно-научную подготовку, включающую в себя специальные разделы математики, а также формирование способности выпускников обеспечивать комплексную безопасность в информационной сфере (практически все отечественные образовательные программы включают разделы, посвященные организационным и правовым, программным и аппаратным, техническим

(инженерно-техническим) и криптографическим методам защиты информации) [16, с.118].

Отдельно следует отметить, что вопросы обеспечения информационно-психологической безопасности граждан и общества, в целом, чаще всего рассматриваются в психолого-педагогическом аспекте. Так, В.П. Поляков, подчеркивает важность проблематики информационной безопасности личности как предмета изучения, а также указывает на важность практической деятельности в сфере отечественного образования и формирования отдельных профилей подготовки по информационной безопасности личности в рамках направлений подготовки, не входящих в блок УГСНП 10.00.00, наряду с существующими программами в области информационной безопасности [80, с.242].

Профессор А.В. Морозов в своих работах также указывает на психолого-педагогическую сущность проблемы, когда объектом информационного оружия становится, прежде всего, сознание и подсознание человека [63, с.287, 65, с.69]. Автор, акцентирует внимание на актуальность и чрезвычайную важность обеспечения информационной безопасности в условиях цифрового образовательного пространства [60, 61, 62, с.221]. Отечественные ученые указывают на необходимость обеспечения информационной безопасности и блокирования возможных рисков в образовательных организациях [60, 62, 63, 86].

Таким образом, мы полагаем, что отдельные аспекты *гуманитарной составляющей информационной безопасности* (такие как обеспечение информационно-психологической безопасности граждан и общества) несколько шире компетенций специалистов в области информационной безопасности (блока 10.00.00 «Информационная безопасность») и, в большей степени, затрагивают психолого-педагогическую область исследований.

### **1.3 Профессиональное образование будущих специалистов по информационной безопасности в Великобритании, США, Германии и Франции**

#### *1.3.1 Система профессионального образования в области информационной безопасности в Великобритании*

Образование по защите информации в Великобритании включает в себя школьную подготовку по вопросам кибербезопасности, высшее и поствысшее образование, а также многочисленные курсы по защите информации для разных возрастных групп: от детей 11 лет до дипломированных бакалавров и магистров.

В 2017 году был открыт Центр национальной кибербезопасности в Лондоне, который стал подразделением правительственной связи страны. С целью устранения нехватки квалифицированных кадров в сфере информационной безопасности, по инициативе Центра, в британских школах появились уроки по кибербезопасности и защите информации, на которых специалисты будут искать будущих экспертов для защиты интересов страны на государственном уровне.

Высшее (программы бакалавриата) и поствысшее (программы магистратуры и программы, дающие дополнительные сертификаты и дипломы) образование по информационной безопасности представлено высшими учебными заведениями Великобритании (колледжи, университеты). Общая схема британской системы уровней подготовки будущих специалистов в области информационной безопасности и укрупненных блоков представлена на рисунке 6.



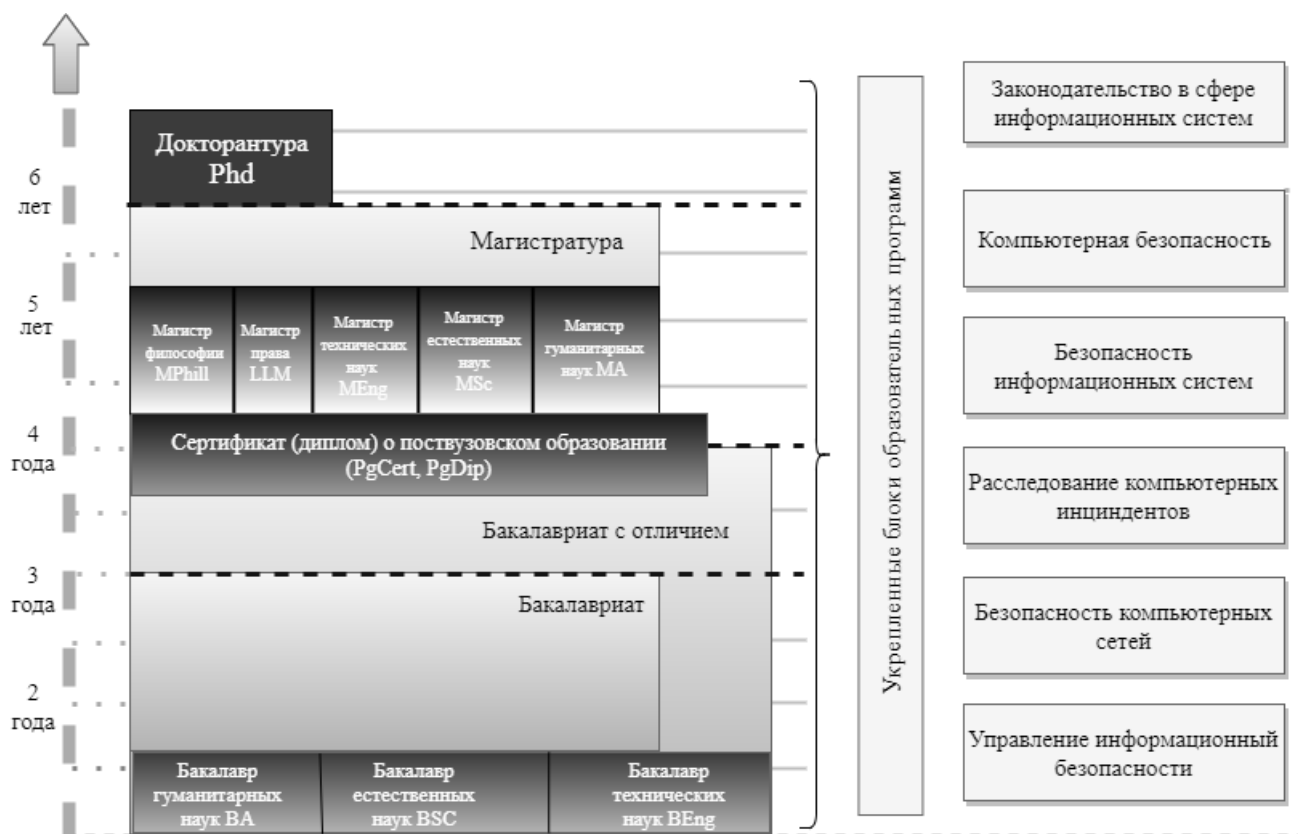


Рисунок 6 – Схема уровней подготовки будущих специалистов в области информационной безопасности и укрупненных блоков в Великобритании.

По программам обучения в области информационной безопасности студенты после 3-х лет обучения имеют возможность получить степень бакалавра, а в случае продолжения обучения еще в течение одного года студенты имеют возможность получить академическую степень бакалавра с отличием [15, с.67].

В ходе исследования системы профессионального образования специалистов по защите информации был проведен обзор образовательных программ Великобритании, опубликованных на официальных интернет-ресурсах образовательных организаций. В итоге мы обнаружили 223 образовательные программы в сфере информационной безопасности, которые реализуют 64 образовательные организации [15, с.67].

Обзор обнаруженных образовательных программ бакалавриата показывает, что в сфере информационной безопасности можно получить одну из трех

степеней высшего образования:

- бакалавр гуманитарных наук (BA);
- бакалавр естественных наук (Bsc);
- бакалавр технических наук (BEng).

Проведенный количественный анализ показывает, что по завершении большинства программ бакалавриата по информационной безопасности выпускники получают степень бакалавра естественных наук – почти 80 %, степень бакалавра гуманитарных наук по информационной безопасности – 17 %. Среди всех рассмотренных программ бакалавриата лишь 3 % заканчиваются присуждением степени бакалавра технических наук.

Поствысшее образование подразумевает любой вид обучения после получения степени бакалавра. Так, за один год после бакалавриата можно получить диплом (PgDip) или сертификат о поствысшем образовании (PgCert), или продолжить обучение в магистратуре. Получить британский диплом магистра по информационной безопасности можно через один или два года, продолжительность обучения зависит от выбранной интенсивности учебного дня и недели.

В сфере информационной безопасности в Великобритании возможно присуждение одной из пяти степеней магистра:

- магистр гуманитарных наук (MA);
- магистр естественных наук (Msc);
- магистр технических наук (MEng);
- магистр права (LLM);
- магистр философии (MPhil).

Аналогично программам бакалавриата, абсолютное большинство программ поствысшего образования заканчиваются получением степени магистра естественных наук – 89 %, 6 % – магистра права, 3 % – магистра философии, по 1 % – магистров гуманитарных и технических наук.

Детальное изучение содержания большого количества разнообразных

программ по информационной безопасности позволило нам выделить несколько укрупненных блоков образовательных программ, представленных на рисунке 7. Образовательные программы, которые имеют схожий набор специализированных дисциплин (тем, модулей) были объединены в общий укрупненный блок.

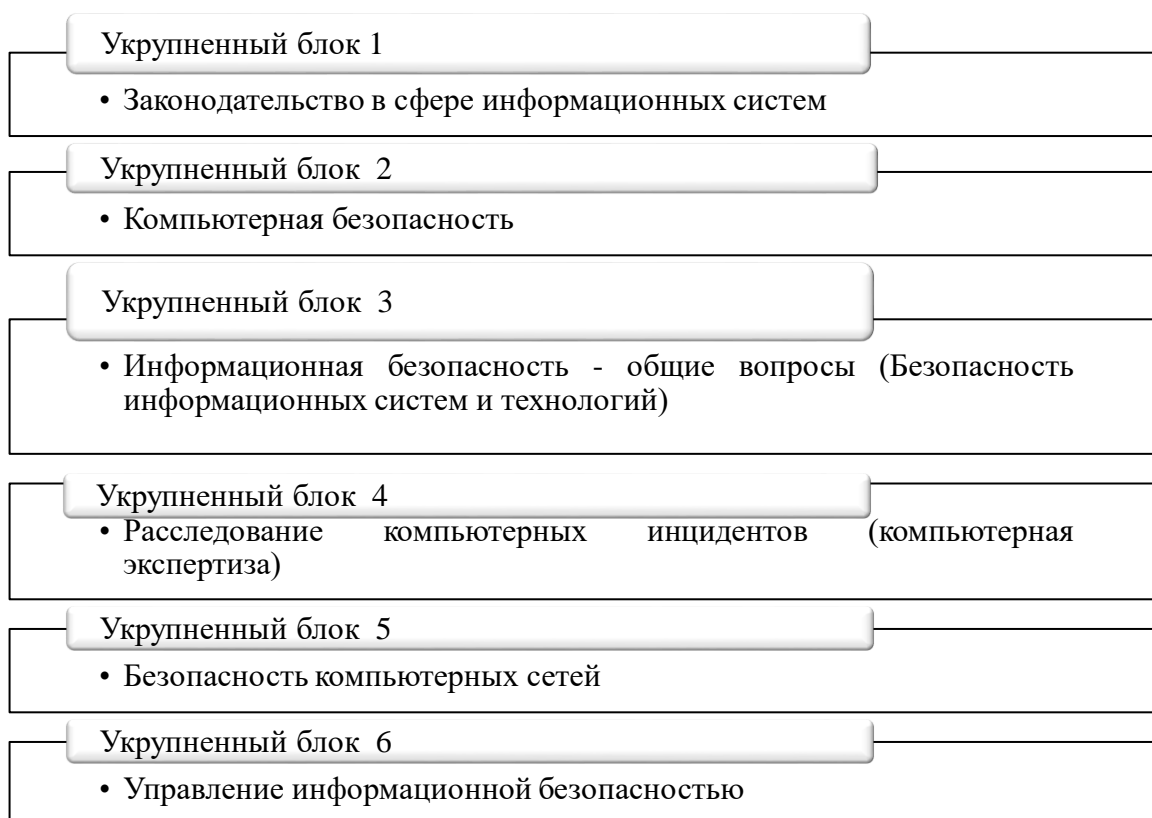


Рисунок 7 – Укрупненные блоки образовательных программ по информационной безопасности в Великобритании.

Рассмотрим образовательные программы бакалавриата и программы поствысшего образования в области информационной безопасности в Великобритании.

На рисунке 8 приведено соотношение числа образовательных программ бакалавриата по укрупненным блокам в Великобритании.

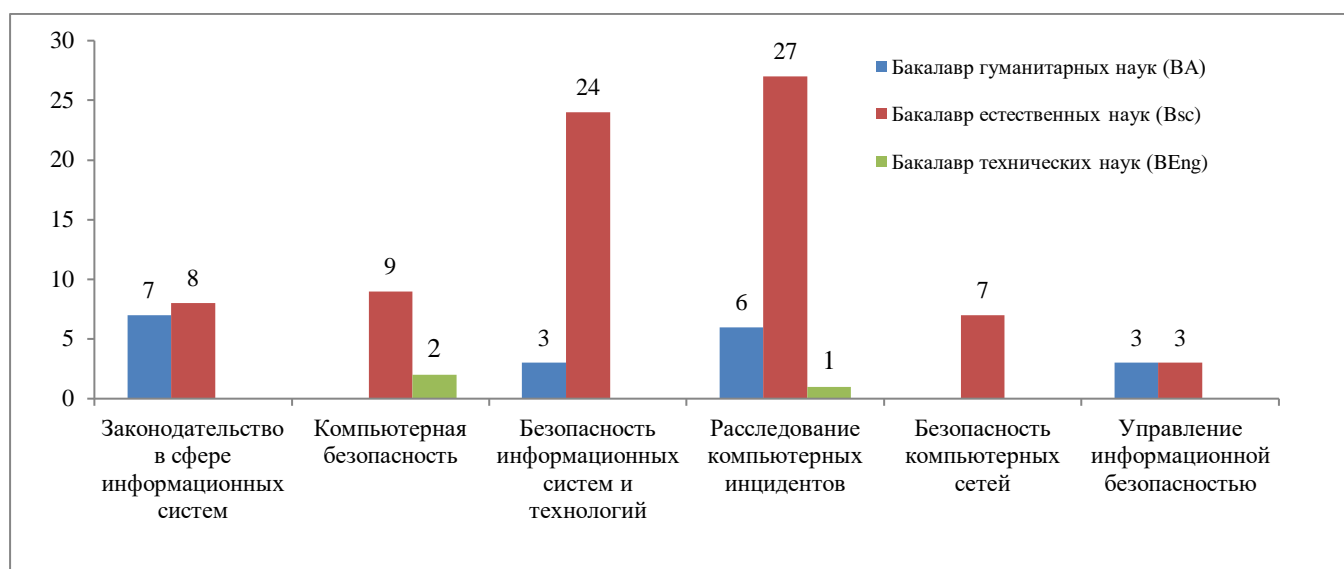


Рисунок 8 – Соотношение числа образовательных программ бакалавриата по укрупненным блокам в Великобритании, %.

В 1-й год обучения бакалавров (на примере разных направлений подготовки специалистов по информационной безопасности Лондонского Университета Метрополитен (London Metropolitan University)) [144] много одинаковых дисциплин, таких как: «Архитектура программных и аппаратных средств», «Введение в Интернет», «Введение в криминологию», «Введение в программирование», «Введение в расследование компьютерных инцидентов» и других. Различия между направлениями подготовки начинаются со 2-го года обучения, когда вуз в учебный план включает дисциплины, специфические только для конкретной образовательной программы.

Проанализируем содержание образовательных программ для нескольких университетов, имеющих образовательные программы, входящие в общий укрупненный блок.

К укрупненному блоку по компьютерной безопасности можно отнести следующие образовательные программы бакалавриата:

- «Компьютерная безопасность», бакалавр технических наук (Computer Security, BEng), Стаффордширский университет [140];
- «Компьютерная безопасность», бакалавр естественных наук

(Computer Security, BSc), Университет Д'Монфорта [141];

– «Компьютерная безопасность и расследование цифровых преступлений», бакалавр естественных наук (Computer Security with Forensics, BSc), Университет Хэфлэлла Халлама [142].

В 1-й год обучения в рассматриваемые программы включены общие дисциплины по программированию, архитектуре компьютеров, вычислительным сетям, основам информационной безопасности. Следует отметить, что дисциплины 1-го года обучения в разных университетах схожие.

Со 2-го года обучения дисциплины в схожих образовательных программах разных вузов заметно отличаются. Среди них встречаются дисциплины по общим вопросам компьютерной безопасности, менеджменту и управления рисками информационной безопасности, безопасности компьютерных сетей, биометрии. Каждый вуз по своему усмотрению и, в зависимости от собственных направлений научных исследований, вводит дисциплины в учебный план.

Необходимо отметить, что каждая программа содержит целый набор дисциплин, связанных с расследованием цифровых преступлений и проведением компьютерной экспертизы. Обучение по всем программам заканчивается защитой дипломного проекта.

Набор образовательных программ, входящих в блок по общим вопросам информационной безопасности (безопасности информационных технологий) представлены в приложении А, среди которых рассмотрены программы [15]:

– «Безопасность информационных систем», бакалавр естественных наук (Information Security Systems, BSc), Университет Восточного Лондона [160];

– «Безопасность информационных технологий», бакалавр естественных наук (Information Technology Security, BSc), Лондонский Университет Метрополитен [166];

– «Компьютерная и информационная безопасность» бакалавр естественных наук (Computer and Information Security, BSc), Университет Хэфлэлла Халлама [130].

Аналогично программам блока «Компьютерная безопасность» в учебный план на 1ом году обучения также включены общие дисциплины по программированию, архитектуре компьютеров, вычислительным сетям, основам информационной безопасности, а со 2го года студенты изучают специализированные дисциплины [6, с.103].

Программы бакалавриата блока по расследованию цифровых преступлений [131, 132, 133] также включают в себя общие дисциплины, связанные с математикой, информационными системами, компьютерными сетями, программированием и другими. Начиная с 1-го года обучения, во все образовательные программы активно вводятся специализированные дисциплины: «Профессиональное расследование компьютерных инцидентов и безопасность», «Расследование и цифровые доказательства», «Введение в криминологию», «Введение в расследование компьютерных инцидентов». Со 2-го года – этот набор дополняется расширенными дисциплинами, например: «Правовые, социальные, этические и профессиональные вопросы», «Законодательство в сфере компьютерных системах», «Компьютерная экспертиза».

Следует отметить наличие в образовательных программах специфичных дисциплин, связанных со сбором доказательной базы: «Техника цифровых исследований», «Цифровой источник доказательств», «Преступление в контексте», «Преступления и технологии». При этом дисциплины, изучающие сбор доказательной базы, идут после изучения технологий расследований компьютерных инцидентов.

Перейдем к рассмотрению следующих образовательных программ блока безопасность компьютерных сетей, к которым относятся:

- «Компьютерные сети и безопасность», бакалавр естественных наук (Computer Networks and Security, BSc), Стаффордширский университет [136];
- «Управление сетями и безопасность», бакалавр естественных наук (Network Management and Security, BSc), Университет Миддлсекса [182];
- «Безопасность компьютерных сетей», бакалавр естественных наук (Computer Network Security, BSc) Вестминстерский университет [135].

Программы по направлению бакалавриата включают в свой учебный план дисциплины по использованию компьютерных сетей (в том числе и беспроводных), основами компьютерной техники, программированию с использованием структур данных и алгоритмов, безопасности информационных систем, криптографии. Много внимания уделяется инжинирингу сетей (маршрутизации) и профессиональной разработке различных сетевых приложений. Особый акцент делается на безопасности сетей и веб-приложений.

Следует отметить, что ряд дисциплин, включенных в образовательные программы блока по безопасности компьютерных сетей, реализуется с использованием вендорских образовательных модулей Сетевой Академии Cisco.

Далее рассмотрим образовательные программы поствысшего образования в области информационной безопасности в Великобритании, в результате успешного окончания которого студенты могут получить сертификат о послевузовском образовании, диплом о послевузовском образовании, либо степень магистра.

На рисунке 9 представлено количественное сравнение числа образовательных программ поствысшего образования в области информационной безопасности в Великобритании, к которым относятся программы с выдачей сертификата о послевузовском образовании и программы с выдачей диплома о послевузовском образовании. Чаще всего встречаются программы по общим вопросам информационной безопасности (что составляет половину от общего числа всех программ), на втором месте по популярности – образовательные программы по расследованию цифровых преступлений.

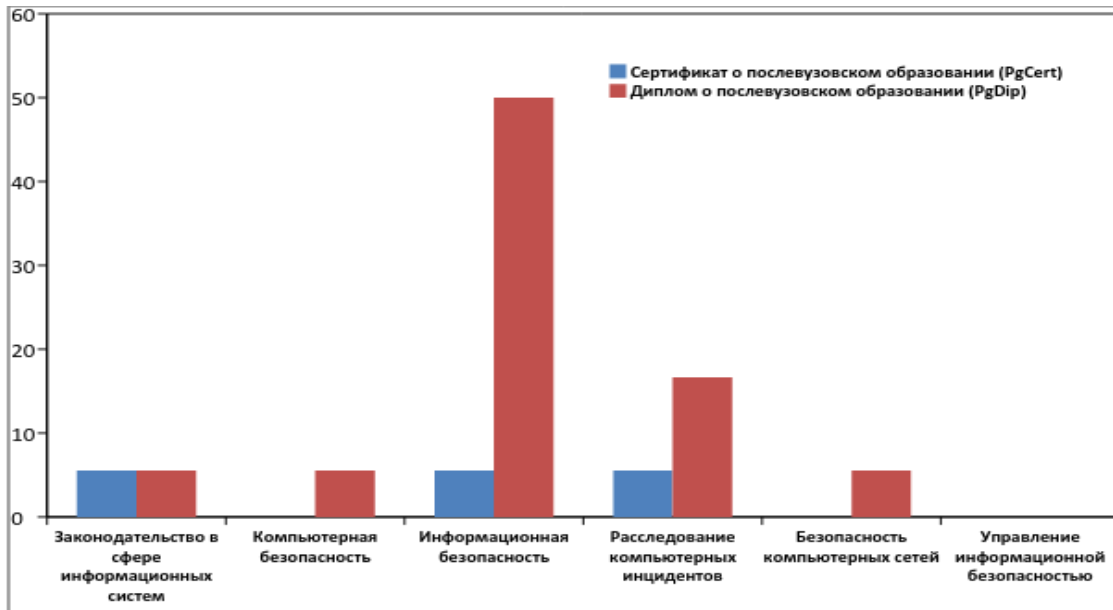


Рисунок 9 – Соотношение количества программ поствысшего образования по укрупненным блокам в Великобритании, %.

На рисунке 10 приведено соотношение количества магистерских программ по укрупненным блокам в Великобритании [6, с.104].

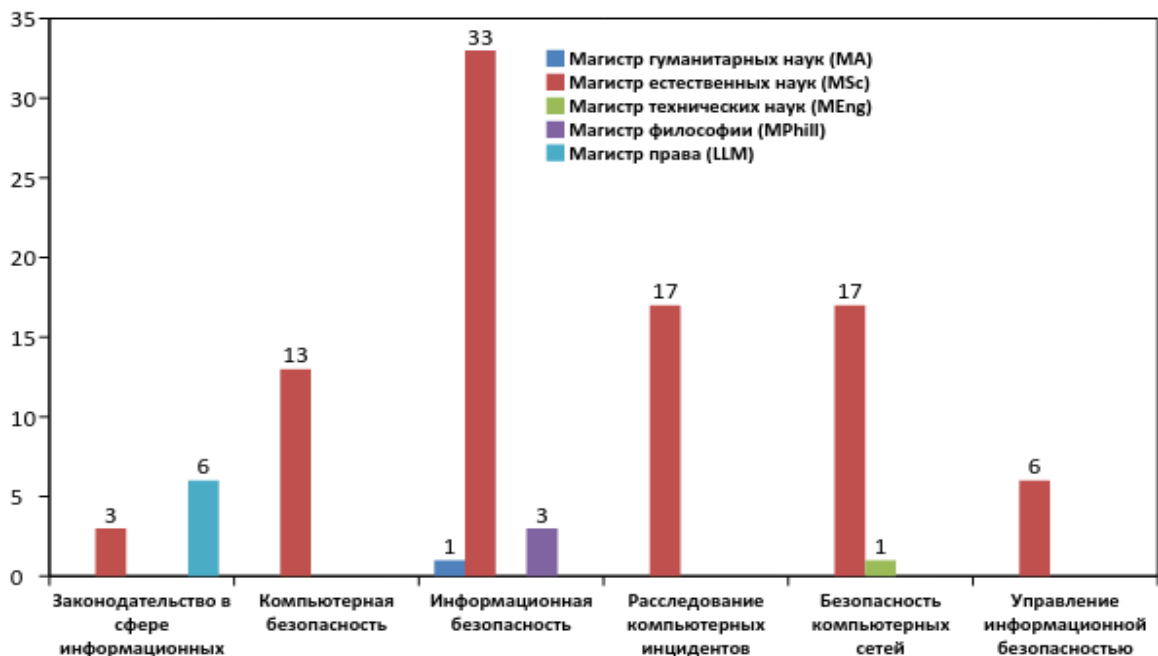


Рисунок 10 – Соотношение количества магистерских программ по укрупненным блокам в Великобритании, %.



Лондонский Университет Метрополитен реализует несколько магистерских образовательных программ [144]:

- «Расследование компьютерных инцидентов», степень магистра естественных наук (Computer Forensics, MSc);
- «Безопасность информационных технологий», степень магистра естественных наук (IT Security, MSc);
- «Управление сетями и безопасность», степень магистра естественных наук (Network Management and Security, MSc);
- «Управление сетями и безопасность», степень магистра технических наук (Network Management and Security, MEng);
- «Управление информационной безопасностью», степень магистра гуманитарных наук (Information Security Management and Governance, MA).

Следует отметить, что Лондонский Университет Метрополитен предлагает две программы магистратуры с одинаковым названием – «Управление сетями и безопасность», но различными присуждаемыми степенями: магистр естественных наук (MSc) и магистр инженерных наук (MEng). При этом программа магистра естественных наук содержит в себе больше дисциплин, чем магистр инженерных наук.

Магистерские программы обучения блока Компьютерная безопасность [139, 148] (с присвоением звания магистр естественных наук) в основном содержат специализированные предметы, направленные на изучение принципов создания надежных сетевых приложений, при этом уделяется внимание профессиональной практике и собственным исследовательским проектам.

К образовательным программам блока Безопасность информационных технологий относятся:

- «Безопасные информационные технологии», магистр естественных наук, (Information Technology Security, MSc), Вестминстерский университет [162];
- «Безопасность информационных систем», магистр естественных наук, (Information Systems Security, MSc), Университет Шеффилда Халлама [161];
- «Безопасность информационных технологий», магистр естественных наук, (Information Technology Security, MSc), Вестминстерский университет [162];

наук, (IT Security, MSc), Лондонский Университет Метрополитен [166].

Магистерские программы содержат дисциплины по безопасности систем и приложений, а также аудиту систем безопасности и компьютерной экспертизе.

Образовательные программы магистратуры блока по расследованию компьютерных инцидентов включают в себя:

– «Расследование компьютерных инцидентов», магистр естественных наук, (Computer Forensics, MSc), Вестминстерский университет [134];

– «Расследование компьютерных инцидентов», магистр естественных наук, магистр естественных наук, (Forensic Computing, MSc), Университет Де Монфорта [153];

– «Расследование компьютерных инцидентов», магистр естественных наук (Forensic Computing, MSc), Стаффордширский университет [152].

Магистерские программы содержат расширенные дисциплины по методам и проблемам криминалистического исследования компьютерных систем, направленных на получение профессиональных навыков.

При анализе образовательных программ блока Безопасность компьютерных сетей обнаружены следующие программы:

– «Компьютерная и сетевая безопасность», магистр естественных наук (Computer and Network Security, MSc), Университет Миддлсекса [137];

– «Безопасность сети», магистр естественных наук, (Network Security, MSc), Университет Англия Раскин [184];

– «Управление сетями и безопасность», магистр естественных наук (Network Management and Security, MSc), Лондонский Университет Метрополитен [183].

Магистерские программы содержат дисциплины по безопасности и качественному обслуживанию компьютерных сетей, по архитектуре и функционированию сетевых систем безопасности, а также управлению систем безопасности.

Результаты анализа образовательных программ бакалавриата и магистратуры в вузах Великобритании подробно представлены в опубликованных

нами статьях [6, 9, 10, 11, 14, 15, 114], что позволяет сделать следующие выводы: образование в сфере защиты информации в Великобритании ориентируется на подготовку кадров, способных обеспечить информационную безопасность, прежде всего, в ее естественно-научной составляющей (проведение компьютерной экспертизы, вопросы программно-аппаратной защиты информации, защита компьютерных сетей), а также гуманитарной составляющей (расследование компьютерных инцидентов, правовая защита информации). Практически не уделяется внимание инженерно-техническим методам обеспечения информационной безопасности.

Все образовательные программы четко ориентируются на узкий круг вопросов защиты информации в той или иной сфере и не предполагают комплексного подхода к формированию безопасного информационного пространства.

### *1.3.2 Система профессионального образования в области информационной безопасности в США*

В США нами было обнаружено более 150 образовательных программ, соответствующих предметной области защиты информации. При этом следует отметить, что все образовательные программы формируются образовательными организациями без учета единых образовательных стандартов.

Система высшего образования США в области информационной безопасности построена следующими ступенями:

1. Уровень бакалавра (Undergraduate Level) предполагает после освоения образовательной программы получение одной из двух академических степеней:

- ассоциат (Associate Degree) – диплом выдается после двух лет обучения;
- бакалавр (Bachelor's Degree) – 1-й полный цикл высшего образования,

диплом выдается после четырех лет обучения.

2. Уровень магистратуры и аспирантуры (Graduate Level). Предполагает одну «промежуточную» квалификацию и две академические степени:

- магистр (Master's Degree) – 1 год;
- специалист (Specialist in Education (Ed.S.)) – 2 года;
- доктор наук (PhD) – 3-4 года.

Анализ содержания образовательных программ США позволил выделить следующие укрупненные блоки (рисунок 11).



Рисунок 11 – Укрупненные блоки образовательных программ по информационной безопасности в США.

Следует отметить, что разнообразие магистерских образовательных программ по информационной безопасности несколько шире, чем программы бакалавриата: в программах бакалавриата не встречаются отдельные направления по экономике и управлению (менеджменту) информационной безопасностью

(рисунок 12). Обучение по данным программам требует наличие базовых знаний по обеспечению безопасности в компьютерных системах и сетях.

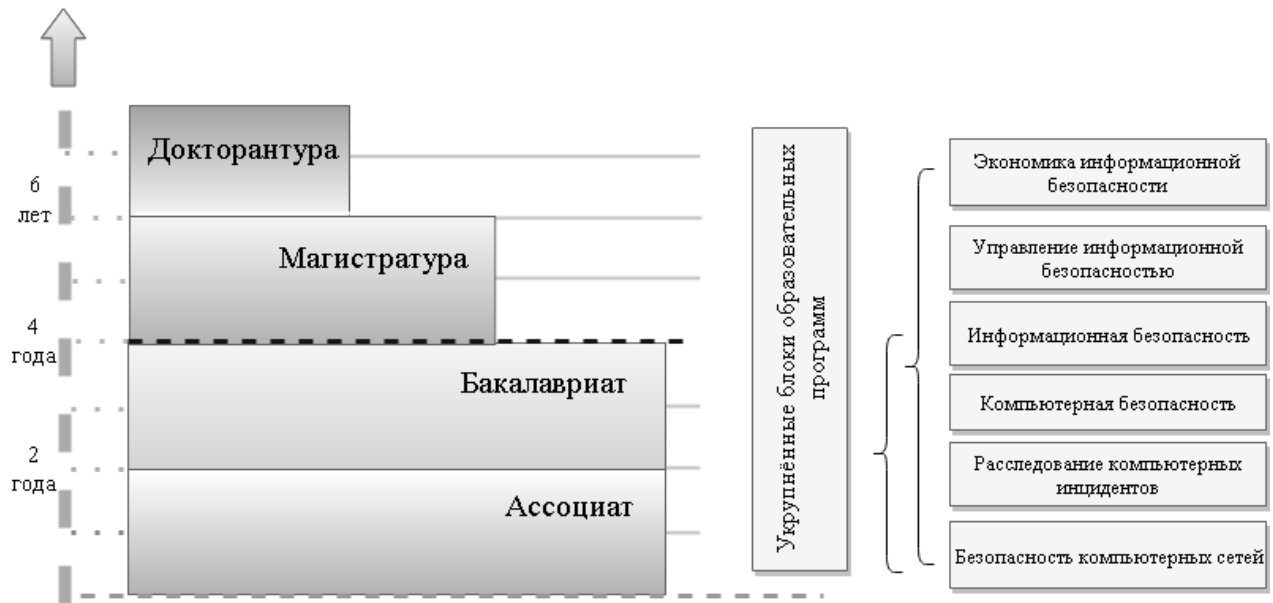


Рисунок 12 – Схема уровней подготовки по ИБ и укрупненные блоки образовательных программ в США.

На рисунке 13 приведено распределение числа образовательных программ бакалавриата по направлениям подготовки в США. Видно, что в наибольшей степени, востребованными образовательными программами являются программы по расследованию цифровых преступлений, по общим вопросам информационной безопасности, компьютерной безопасности и безопасности сетей [113, с.128].

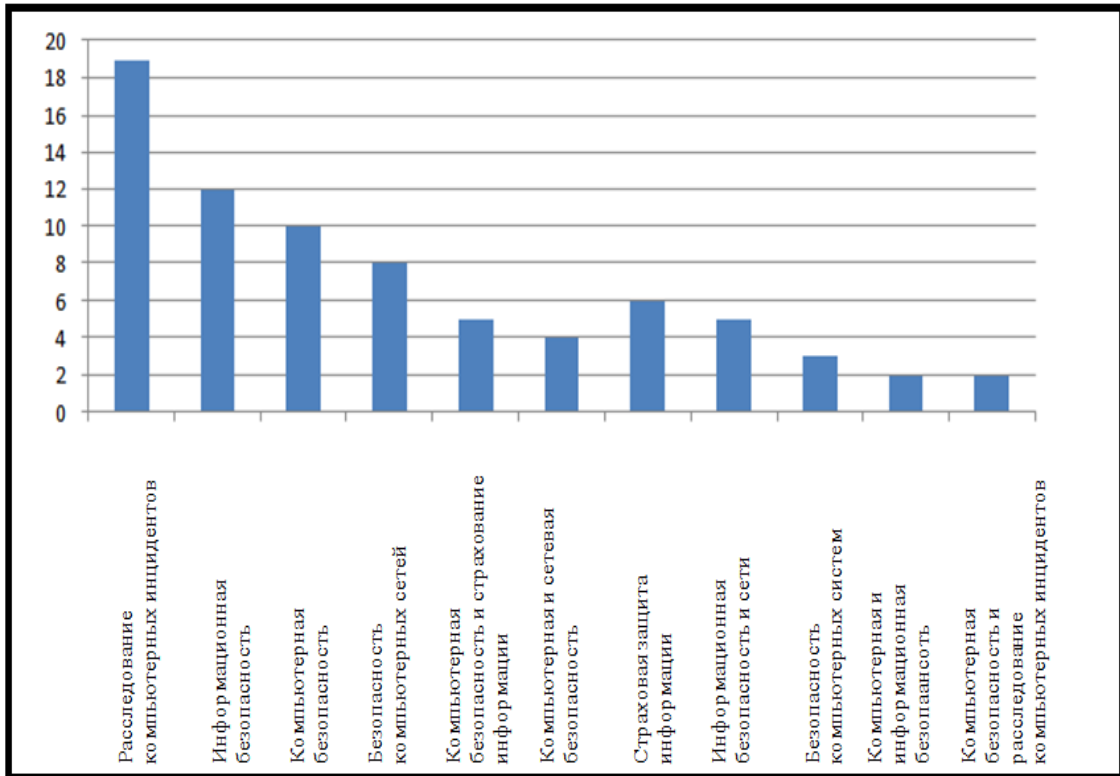


Рисунок 13 – Соотношение количества образовательных программ бакалавриата по направлениям подготовки в США, %.

Один из примеров образовательных программ по общим вопросам информационной безопасности приведен в приложении Б (университета города Чаттануга) [197, 203]. В приложении представлены цели, задачи и содержание отдельных специализированных дисциплин. Следует отметить, что дополнительно с учебными дисциплинами университета, студенты имеют возможность пройти дополнительные курсы и получить профессиональные сертификаты, подтверждающие их профессионализм [113, с.129].

В приложении В приведено распределение образовательных программ магистратуры по выделенным укрупненным блокам.

На рисунке 14 приведено распределение количества образовательных программ подготовки магистров по укрупненным блокам в США. Диаграмма демонстрирует, что к самым популярным и многочисленным магистерским образовательным программам относятся программы по общим вопросам информационной безопасности, а также по компьютерной безопасности и

управленческим аспектам информационной безопасности.

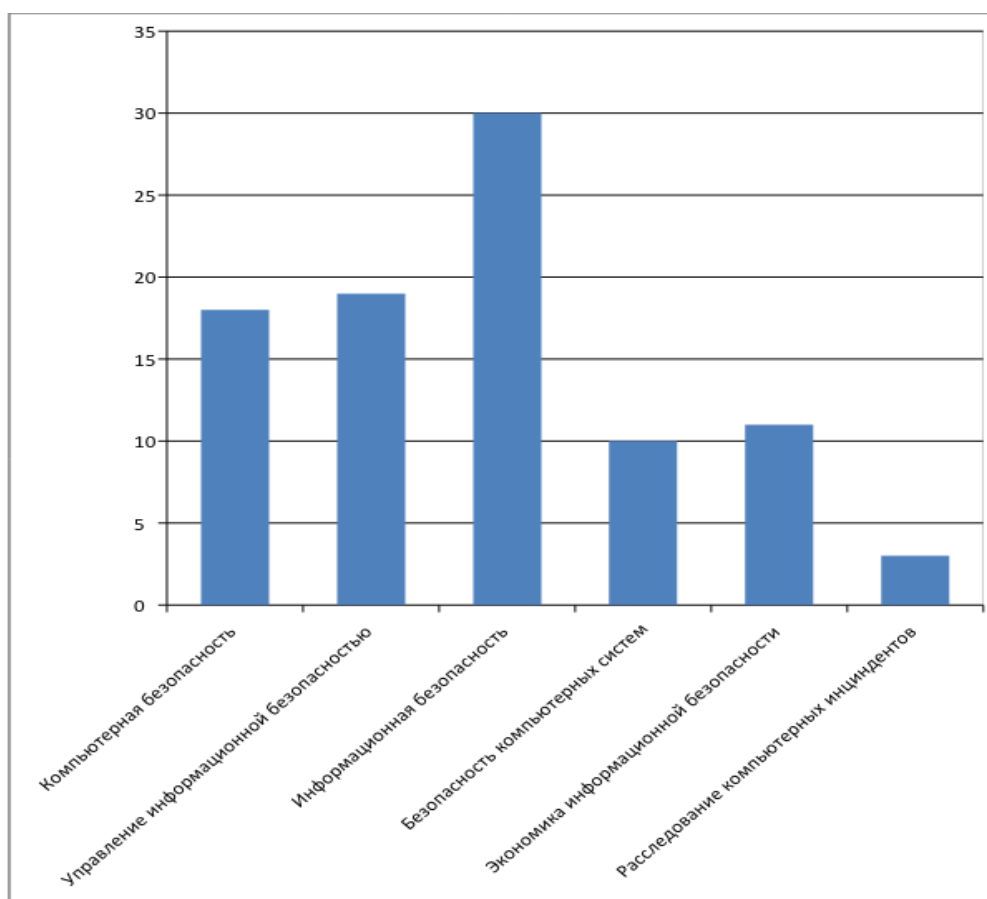


Рисунок 14 – Соотношение количества образовательных программ магистратуры по направлениям подготовки в США, %.

Образовательные программы магистратуры укрупненного блока по общим вопросам информационной безопасности реализуют следующие образовательные организации: Технический университет штата Колорадо, Университ Д'Паул, Университет штата Пенсильвания в Восточном Страдсбурге, Институт Технологий в городе Джорджия, Университет Блумингтон штата Индианы, Университет Джона Хопкинса, Университет штата Кентукки, Университет Системы Знаний (Knowledge Systems Institute), Университет Маршал, Университет Роберта Мориса, Институт технологий Стивенсон, Университет в городе Тусон, Университет передовых технологий, Университет в городе Хьюстон, Университет штата Канзас и других.

Магистров по направлениям блока по компьютерной безопасности готовят в следующих университетах: Университет Бредли, Технический университет штата

Колорадо, Технический университет Лоуренс, Университет в городе Нью-Джерси, Институт технологий в городе Нью-Йорка, Университет Стайер, Университет в городе Тусон, Университет штата южной Калифорнии.

Магистров по направлениям блока по управлению информационной безопасностью готовят в следующих университетах: Университет в городе Белвью, Университет Бенедикт и других.

Магистров по направлениям блока безопасности компьютерных сетей готовят в университетах: Университет Кларк штата Антланта, Университет Д'Врай, Университет Джорджа Мэсона, Университет Джорджа Вашингтона, Северо-западный Политехнический Университет, Питтсбургский университет.

Магистров по направлениям блока по экономике информационной безопасности готовят в университетах: Колледж Анна Мария, Университет в городе Белвью, Университет Брендмэн, Университет штата Калифорния, Университет Д'Врай, Университет Феррис, Университет Джэймса Мэдисона, Международный университет Веббер.

Магистров по направлениям блока по расследованию компьютерных инцидентов готовят, в том числе, в университетах: Университет центральной Флориды, Университет Джорджа Мэсона, Университет Пердью.

В приложении Г представлено краткое описание и содержание специализированных дисциплин образовательной программы по Информационной безопасности, которую реализует колледж Мерси [177]. Следует отметить, что в рамках реализации образовательной программы также предусмотрена дополнительная профессиональная сертификация будущих специалистов [113, с.131].

Результаты анализа образовательных программ бакалавриата и магистратуры [124, 129, 155, 169, 172, 177, 179, 189, 190, 191, 192, 193, 196, 197, 198, 203] в вузах США подробно представлены в опубликованных нами статьях [6, 9, 10, 13, 14, 113, 114], что позволяет сделать следующие выводы: образование в сфере защиты информации в США ориентируется на подготовку кадров, способных обеспечить информационную безопасность, в большей степени,



*естественно-научной* составляющей (изучается большое количество тем по расследованию цифровых преступлений, программно-аппаратным методам защиты информации, обеспечению безопасности компьютерных сетей), а также *гуманитарной* (расследование цифровых преступлений, правовые методы защиты информации) составляющей информационной безопасности; при этом *технической* сфере уделяется мало внимания. Рынок трудоустройства выпускников, прежде всего, в бизнес-структурах.

### *1.3.3 Система профессионального образования в области информационной безопасности в Германии*

В системе немецкого образования, представленной и государственными, и частными образовательными учреждениями, нами было обнаружено 10 образовательных программ по информационной безопасности.

В немецких университетах студент после освоения программы, связанной с вопросами информационной безопасности, может получить академические степени: бакалавра (Bachelor/Bakkalaureus) и магистра (Master). Обучение по программам бакалавриата в области информационной безопасности, в основном, длится три года (иногда четыре), по программам магистратуры – один-два года [28]. После завершения магистратуры выпускник может продолжить исследовательскую деятельность по программам докторантуры (рисунок 15).

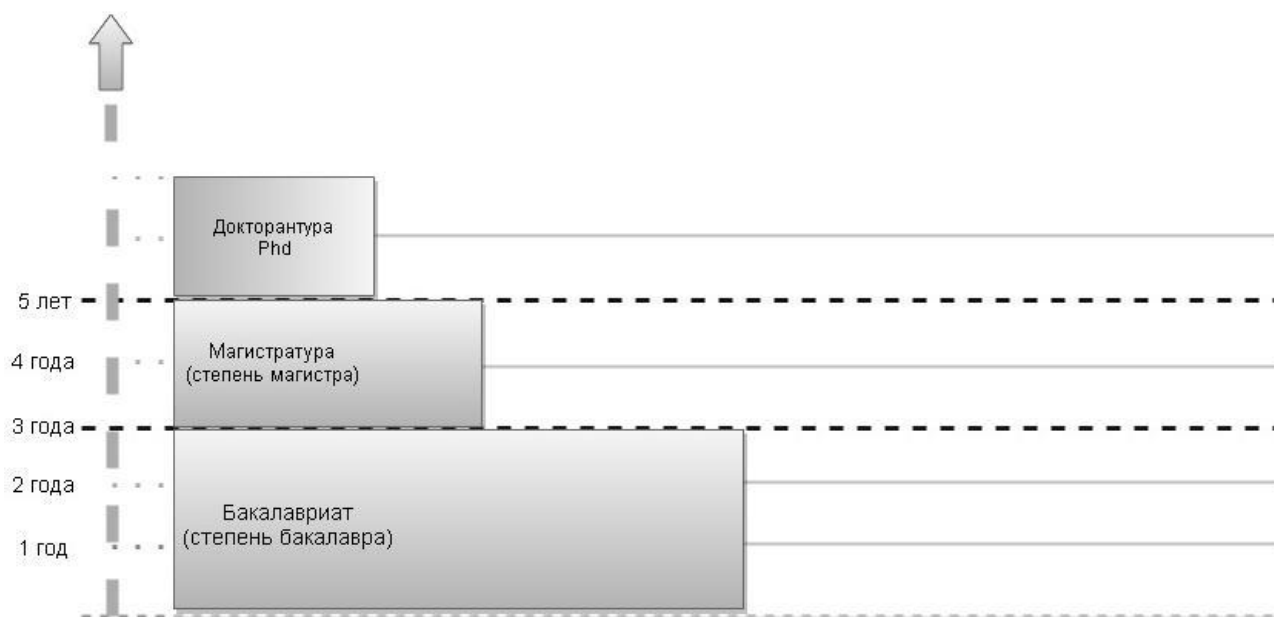


Рисунок 15 – Общая схема ступеней профессионального образования специалистов по информационной безопасности в Германии.

В рамках обучения по программам бакалавриата в области информационной безопасности студент на начальном этапе (1-3-й семестры) изучает основы информатики, алгоритмизации и программирования, защиты информации, а также вырабатывает навыки научно-исследовательской работы. Основной период обучения длится в течение трех-четырех семестров, когда студент занимается углубленным изучением выбранных специализированных дисциплин предмета, а также проводит самостоятельные исследования, которые в дальнейшем становятся основой выпускной работы. 6-й семестр выделен для работы над дипломным проектом на соискание академической степени бакалавра, а также для подготовки к сдаче итоговых экзаменов.

Программы магистратуры, в большей степени, посвящены научно-исследовательской работе студентов и изучению дисциплин продвинутого уровня.

Среди немецких образовательных программ нами были обнаружены программы бакалавриата по информационной безопасности в университетах в городе Ален, в городе Оффенбург, а также Ганноверском университете имени

Лейбница и Боннском университете [116, с.79; 159; 163; 167; 204].

Рассмотрим подробнее образовательную программу бакалавриата «Корпоративная и информационная безопасность» университета прикладных наук в городе Оффенбург [150, 151]. Образовательная программа готовит будущих специалистов, способных обеспечивать информационную безопасность в сфере бизнеса.

К компетенциям выпускника относятся:

- способность использовать ноу-хау в области современных компьютерных технологий и информатики;
- способность проводить экспертизы в области информационной безопасности и новых средств массовой информации;
- способность интеллектуального управления бизнесом;
- способность управления проектами;
- способность разрабатывать, настраивать и эксплуатировать безопасные компьютерные сети, на основе детального знания современного программного обеспечения, компьютерных и сетевых технологий;
- способность применять методы и инструменты для оценки уязвимостей компьютерных систем;
- способность разрабатывать безопасное программное обеспечение для ИТ-систем.

**Формы проведения практических занятий.** Студенты обучаются с использованием программного обеспечения в области обработки данных и процессов безопасности, информационных технологий обеспечения механизмов безопасности и их интеграции в корпоративный технологический процесс. Квалификация выпускника подразумевает профессиональное использование программного обеспечения в соответствии с требованиями безопасности компаний. Кроме того, много времени отводится практической организации управления системой безопасности, законодательству. Во время всего обучения практические занятия строятся на работе в команде (группы студентов

работают в лабораториях, стажируются, участвуют в семинарах).

**Квалификация выпускника.** Приобретенные знания и навыки обеспечивают выпускников условиями занятости и позволяют:

- выступать в качестве разработчика концепции безопасности сетевой системы (интернет, интранет, экстранет);
- выступать в качестве эксперта по расследованию и сбору доказательной базы компьютерных преступлений;
- иметь руководящие должности, как в отделах безопасности, так и общие руководящие должности в компаниях;
- выступать в качестве администратора систем безопасности для всех типов онлайн-услуг, электронной коммерции, банков, интернет-провайдеров, государственных и военных организаций;
- быть разработчиком информационных систем для обработки конфиденциальных данных;
- быть экспертом в быстро развивающейся области консалтинга информационной безопасности, например, бизнес-сертификации по стандартам ISO 27001, BSI и других;
- выступать как эксперт по вопросам информационной безопасности и ее сетевой архитектуры;
- выступать в качестве системного инженера или разработчика программного обеспечения информационной безопасности, системного администратора в сфере безопасности.

**Практики и стажировки.** Стажировка студентов проходит в различных компаниях, работающих в области информационной безопасности и имеющих богатый опыт в данной области. Практика является неотъемлемой частью подготовки, где подтверждаются знания, полученные в университетских лабораториях. По сути, стажировка является «бизнес-практикой», которая включает в себя не только фактическую стажировку, но и зачастую позволяет налаживать важные контакты и начать карьеру после окончания учебы. Задачи стажировки заключаются в решении комплекса технических, организационных

и экономических проблем, в числе которых планирование и проведение мероприятий по информационной безопасности, разработка концепции политики безопасности, проектирование и разработка безопасного программного обеспечения, а также анализ приложений с точки зрения их безопасности.

**Выпускная работа.** Выпускная работа бакалавра является заключительным исследованием студента. Задачами выпускной работы бакалавра являются постановка проблемы, разработка и реализация проекта методами и средствами информационной безопасности. Дипломная работа является научным исследованием с применением теоретических и практических знаний, научных методов. Документация по работе бакалавра должна охватывать все основные аспекты выпускной работы и быть составлена в соответствии с научными критериями. Темы могут быть предложены научным руководителем студента или являться заказом внешних организаций или компаний.

**Учебный план.** Программа бакалавриата имеет длительность в шесть семестров. Изучение курса предполагает модульную структуру (каждый курс является частью модуля), занятия проходят в форме лекций и практических или лабораторных работ. Изучение дисциплины завершается в течение одного семестра с прохождением итогового тестирования. Для оценки прохождения модулей, как и в большинстве вузов Европы, используется система кредитных пунктов. Описание некоторых специализированных дисциплин данной образовательной программы представлено в приложении Д.

Подготовка магистров по информационной безопасности в Германии ведется в образовательных организациях: Ганноверском университете имени Лейбница, Технологическом университете в городе Карлсруэ, Бременском университете, Университете в городе Пассау и других [116, с.81; 125; 164; 170; 174].

В приложении Е приведено описание некоторых специализированных дисциплин образовательной программы бакалавриата со специализацией по информационной безопасности Боннского университета [158].

Рассмотрим подробнее направление подготовки магистров по информационной безопасности (Master of Science) университета в городе Пассау.

При реализации данной образовательной программы применяются традиционные формы обучения (лекции, консультации, семинары). Вместе с тем в рамках программы свойственно организовывать работу студентов в небольших группах для выполнения совместных проектов, заказчиками которых могут быть как вуз, так и сторонние организации.

В конце обучения должна быть подготовлена научная диссертация магистра. Время работы над диссертацией составляет шесть месяцев. Цель, задачи и практическая значимость работы выбираются руководителем магистранта и должны соответствовать области информационной безопасности. В диссертацию могут включаться результаты групповой работы над определенным проектом, в этом случае вклад конкретного выпускника должен быть четко понятен и прописан.

**Возможности для карьерного роста.** Образование, полученное в магистратуре, формирует опытных квалифицированных специалистов области информационной безопасности и дает возможность для карьерного роста в высокотехнологичных областях деятельности, таких как, промышленность, торговля, страхование, предоставление услуг, компании бизнес-консалтинга, органы государственного управления, научные организации.

В приложении Ж представлено описание дисциплин образовательной программы магистратуры «Управление безопасностью», реализуемая университетом прикладных наук в городе Бранденбург [194]. Образовательная программа реализуется в течение трех семестров. В блок базовых дисциплин входят: «Управление безопасностью», «Безопасность информационных технологий», «Основы математических и физических наук», «Право и бизнес-администрирование». Дополнительные дисциплины по выбору: «Социальные науки», «Безопасность для мобильных систем», «Интернет-преступления», «Компьютерная криминалистика». В дополнение к

базовым и обязательным дисциплинам предлагаются следующие дисциплины по выбору: «Видеоанализ в сфере безопасности», «Экспертиза информационных технологий», «Технические аспекты компьютерной экспертизы», «Методологические оценки и сертификации систем защиты», «Управление рисками информационной безопасности», «Личная безопасность», «Физическая безопасность банков», «Новые тенденции в идентификации: философия, техническая реализация и приложения», «Защита информации в экономике».

Краткое описание специализированных дисциплин (в том числе, «Основы управления безопасностью», «Безопасность сети», «Основы безопасности коммуникационных технологий», «Криптология», «Право»), изучаемых в 1-м семестре, приведены в приложении Ж.

Во 2-м семестре изучаются дисциплины:

- «Безопасность и регулирование кризисов. Международный контекст»;
- «Рабочее место специалиста по управлению безопасностью»;
- «Управление сетевой безопасности»;
- «Развитие безопасных информационных систем»;
- «Управление персоналом»;
- производственная практика.

В третьем семестре студенты проходят факультативы для раскрытия практических вопросов управления безопасностью в компаниях и организациях, принимают участие в мастер-семинарах. Обучение заканчивается написанием и защитой магистерской диссертации.

Результаты анализа образовательных программ бакалавриата и магистратуры в вузах Германии подробно представлены в опубликованных нами статьях [6, 14, 17, 114, 116], что позволяет сделать следующие выводы: немецкая система профессионального образования специалистов по информационной безопасности нацелена на формирование у будущих специалистов по защите информации способности решать задачи естественно-

научной составляющей информационной безопасности (криптографическая и программно-аппаратная защита информации) и гуманитарной составляющей (превалируют направления подготовки и дисциплины в них по правовому обеспечению информационной безопасности, страхованию информации, управлению информационной безопасностью). Содержание профессиональной подготовки специалистов в сфере обеспечения безопасности информации в Германии не ориентированы на обеспечение технической (инженерно-технической) защиты информации. Рынок трудоустройства выпускников-специалистов по информационной безопасности – это, в основном, бизнес-структуры, в том числе в промышленности, страховании, торговли и т.п.

#### *1.3.4 Система профессионального образования в области информационной безопасности во Франции*

Французские академические степени в системе высшего образования отличаются от классической англо-саксонской модели бакалавриата и магистратуры, которые приняты в вышерассмотренных зарубежных странах (Великобритания, США, Германия). Французский диплом бакалавра – это аттестат о среднем (школьном) образовании [74]. Система высшего образования состоит из нескольких ступеней: лицензиата, магистратуры и докторантуры (рисунок 16).

В свою очередь, программы лицензиата делятся на «короткий» и «длинный» циклы. «Короткий» цикл, как правило, длится два года и аналогичен русскому среднему профессиональному образованию. Образовательные программы лицензиата «длинного» цикла составляют три года и завершаются получением профессиональной лицензии.



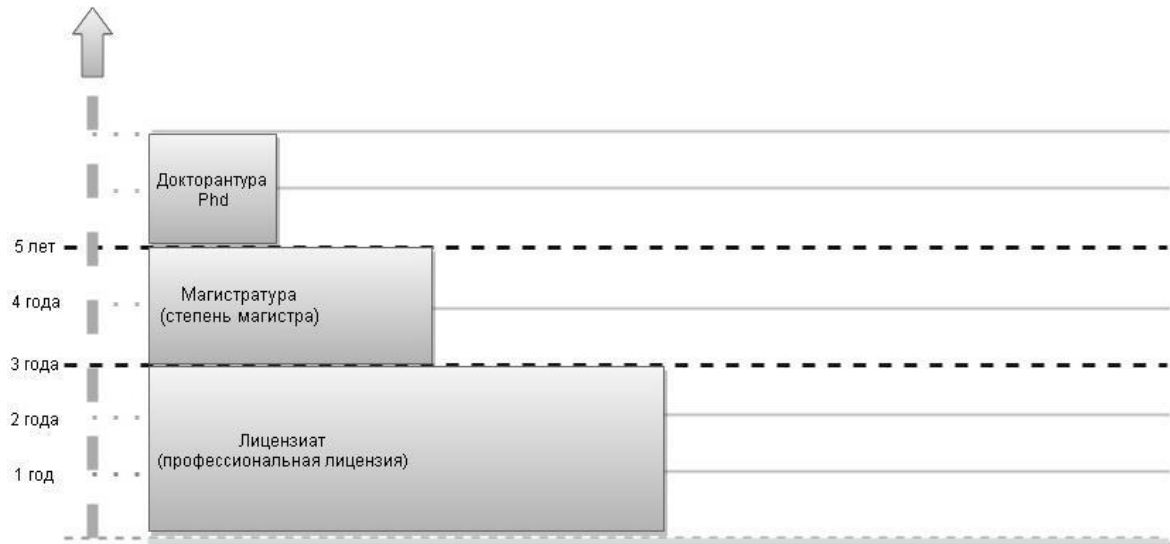


Рисунок 16 – Схема присуждаемых во Франции дипломов о высшем образовании.

Нами были обнаружены всего две образовательные программы по информационной безопасности с присуждением профессиональной лицензии в рамках «длинного» цикла. В основном, среди программ по защите информации реализуются программы магистратуры. В свою очередь, в магистратуру по информационной безопасности поступают, чаще всего, выпускники лицензиата по математике или информатике.

Всего было обнаружено 10 организаций, реализующих образовательные программы по информационной безопасности. Специалистов по защите информации обучают в образовательных организациях, среди которых: университеты в городах Бордо, Ренн, Лимож, Лион, в Высшей школе менеджмента IAE Aix, в Высшей школе Телеком Британь и других [6, с.106-107; 146, 147, 175, 176, 201, 202]. Пример одной из французских образовательных программ магистратуры по компьютерной безопасности, реализуемой университетом города Лимож, представлен в приложении И.

Результаты анализа образовательных программ профессиональной лицензии и магистратуры в вузах Франции подробно представлены в опубликованных нами статьях [6, 14, 114, 115], приводят к выводу о том, что цель профессионального образования будущих специалистов по

информационной безопасности – это формирование способности решать вопросы естественно-научной и гуманитарной составляющей информационной безопасности. Причем, значительное внимание уделяется естественно-научной составляющей, а именно вопросам криптографии. Во французских вузах готовят выпускников, готовых решать задачи защиты информации, как в государственных, так и в частных структурах. Причем акцентируется внимание на государственном секторе, что имеет общие черты с российским профессиональным образованием по информационной безопасности.

#### **1.4 Анализ отечественного и зарубежного опыта по интеграции образовательных программ с вендорскими образовательными курсами и вендорнезависимой сертификацией**

Положительным опытом некоторых зарубежных образовательных программ можно считать то, что после получения степени бакалавра или магистра в рамках направлений подготовки по информационной безопасности, а также во время обучения, студенты имеют возможность прохождения профессиональной сертификации. Подобные сертификации увеличивают конкурентоспособность выпускников на рынке труда. Зачастую в аннотации к зарубежной образовательной программе по информационной безопасности вуз указывает, на какую профессиональную сертификацию ориентируется данная программа [112, с.145].

В настоящее время существует достаточно большое количество программ профессиональной сертификации специалистов по защите информации во всем мире, включая США, Великобританию, Германию и Францию, которые предлагают общественные или профессиональные организации, ИТ-компании, высшие учебные заведения (как государственные, так и частные) [154, с.67].

Образовательная программа вуза обеспечивает прочную основу теоретических знаний и базовых навыков обучающихся, а динамичность индустрии информационных технологий и защиты информации диктует постоянную необходимость актуализации содержания программ дисциплин в соответствии с новыми технологиями, средствами и методами обеспечения информационной безопасности. Профессиональное сообщество через механизм сертификации (и подготовки к ней) обеспечивает необходимую актуализацию содержательного компонента, охватывает современные средства и методы защиты информации, передовой опыт, установленный и востребованный в профессиональной среде.

Существует два основных вида сертификации ИТ-специалистов и

специалистов по защите информации в зависимости от того, какая коммерческая или общественная организация является учредителем данной сертификации. Первую из них – *вендорскую* – проводят «крупные компании с известной торговой маркой, имеющие свои линейки сертификации, соответствующие специфике работы с продуктами и технологиями данной компании» [92, с.151]. Другой вид профессиональной сертификации – *вендорнезависимая сертификация*, то есть не зависящая от конкретного вида информационного продукта, средства по защите информации [112, с.146].

Вендорнезависимая сертификация представляет собой стандартизированный способ оценки компетенций будущих сотрудников работодателями. Как отмечают зарубежные авторы [156, с.31], сертификат является одним из наиболее ценных документов для оценки сформированного уровня готовности выпускников к профессиональной деятельности и дальнейшего развития карьеры в сфере информационной безопасности. Согласно исследованиям заработной платы ИТ-кадров в США, наличие профессионального сертификата повышает годовой заработок в среднем на 9 000 долларов. Другое исследование показало, что прохождение конкретной сертификации – сертификации специалиста по безопасности информационных систем (CISSP) – может увеличить доход на 21 000 долларов в год [156, с.31].

На основе анализа данных о заработной плате специалистов по защите информации Анджей Я. Галински [154, с.71] перечисляет наиболее востребованные сертификаты на профессиональном уровне, которые охватывают вопросы тестирования компьютерных систем и сетей на уязвимость и проникновение, обнаружение угроз, написанию безопасного кода и предотвращение атак, к которым относятся:

- CompTIA Security + (сертификат безопасность +) от CompTIA;
- СЕН: Certified Ethical Hacker (сертификат по этическому хакингу) и ЕССА: Certified Security Analyst (сертификат аналитика по безопасности) от EC-Council;
- CFCE (сертификат судебного компьютерного эксперта) от IACIS;
- GIAC Security Essentials (сертификат по основам безопасности) от SANS;

– CISSP (сертификат специалиста по безопасности информационных систем) от ISC2;

– CISA (сертификат аудитора информационных систем) и CISM (сертификат менеджера по информационной безопасности) от ISACA.

Компания CompTIA – является ведущим мировым поставщиком вендорнезависимых сертификатов в области информационных технологий и информационной безопасности [154, с.71]. В области компьютерной безопасности одним из популярных сертификатов является всемирно признанный и надежный сертификат начального уровня Comp-TIA Security+, который охватывает основы безопасности компьютерных сетей и управления рисками, криптографии, управления идентификацией и систем безопасности. Comp-TIA Security+ оценивает компетенции в широком объеме знаний [173, с.23], необходимые для осуществления профессиональной деятельности в любой отрасли и не имеет требований к опыту работы. Следовательно, такой сертификат имеют возможность получить выпускники или студенты старших курсов.

Вместе с тем, для сертификации по другим программам компании (например, CompTIA Network +) рекомендуют иметь как минимум 2х летний опыт работы в сфере администрирования компьютерных сетей. А сертификат продвинутого уровня – CASP (Advanced Security Practitioner) требует не менее 10 лет опыта работы с информационными технологиями, включая 5-летний опыт в сфере защиты информации.

Международная некоммерческая организация ISACA предлагает сертификаты и практические рекомендации в информационных системах и защиты информации. ISACA располагает двумя видами сертификатов – CISA и CISM. Сертификация CISA – самая популярная для области профессиональной деятельности в сфере аудита и управления рисками. Для ее прохождения недостаточно иметь базовое образование в области информационной безопасности, но также необходим опыт [40]. CISM – прежде всего, управленческая сертификация, в которой все вопросы обеспечения информационной безопасности рассматриваются с позиции менеджмента и

бизнеса. При этом для получения такого сертификата необходимо подтвердить свой 5-летний опыт работы в области информационной безопасности, включая 3х-летний управленческий опыт [41].

Ряд зарубежных университетов, реализующих образовательные программы бакалавриата или магистратуры по информационной безопасности являются партнером организации ISACA, а их выпускники имеют некоторые преимущества при сертификации (а именно, наличие диплома образовательной организации-партнера может быть засчитано выпускнику за 1 год опыта работы в данной сфере).

Отдельно стоит остановиться на сертификации CISSP Международного консорциума по сертификации в области безопасности информационных систем ISC2. Некоторые зарубежные исследователи называют CISSP лучшей сертификацией по кибербезопасности [126, с.1]. Для получения такого сертификата также необходим 5-летний опыт работы, поэтому его уровень не доступен для студентов или выпускников университетов. Многие зарубежные образовательные организации для того, чтобы повысить конкурентоспособность и привлекательность своих образовательных программ по информационной безопасности приглашают к реализации преподавателей, имеющих данный сертификат. Поскольку он имеет широкий охват областей безопасности, CISSP во многих случаях является самым популярным сертификатом для преподавателей [127, с.51].

Помимо вышеперечисленных, в мире существуют достаточно большое количество вендорнезависимых сертификаций различных профессиональных ассоциаций или организаций.

Профессиональная сертификация специалистов по защите информации в России в настоящий момент находится в стадии разработки и регулируется указом Президента РФ № 249 «О Национальном совете при Президенте Российской Федерации по профессиональным квалификациям» от 16.04.2014 г., распоряжением Правительства РФ. № 2042-р «О центре профессиональной подготовки, переподготовки и повышения квалификации рабочих кадров» от

29.09.2016 г., федеральным законом №238 «О независимой оценке квалификации» от 03.07.2016 г., а также рядом нормативно-правовых документов РФ.

В соответствии с докладом рабочей группы (в которую входят представители ФУМО) по оценке квалификации по защите информации и информационной безопасности [22], деятельность в этом направлении должна начаться, в том числе, с «подготовки к организации профессионального экзамена». Разработка квалификаций и фондов оценочных средств будет четко ориентироваться на обобщенные трудовые функции соответствующих профессиональных стандартов.

Однако на данный момент не планируется использовать эти сертификации в рамках реализации основных образовательных программ высшего образования по информационной безопасности. Подобная сертификация будет использоваться для подтверждения квалификации действующих специалистов, имеющих некоторый стаж работы в соответствующих должностях, и, возможно, в рамках дополнительного профессионального образования. Вероятно, в будущем будет вестись работа по внедрению профессиональной сертификации в образовательные программы вузов как следствие гармонизации образовательных и профессиональных стандартов.

Аналогичную точку зрения (относительно важности сертификации выпускников) высказывают В.Н. Соляной и соавторы: «обязательная сертификация должна реализовываться как для выпускников вузов, так и для лиц, окончивших переподготовку кадров по информационной безопасности» [93, с.198].

Некоторые отечественные эксперты по информационной безопасности полагают, что, так как отечественная система вендорнезависимой сертификации находится на начальном этапе разработки, в России с целью подтверждения квалификации специалистов в настоящее время целесообразно использовать зарубежные сертификаты [35].

В комментариях к статье А.В. Лукацкого «Нужен ли CISSP в России?» генеральный директор учебного центра «Микроинформа» делает акцент на

важности сохранения использования международной сертификации в России [54]. При этом добавляет: «...это не имеет никакого отношения к предложению автора вводить в России самостоятельные сертификации по рассматриваемой проблеме».

Резюмируя вышеизложенное, нужно сказать, что система профессиональной сертификации является важным инструментом подтверждения квалификации специалиста. На данный момент отечественной системы оценки квалификации не существует, но ведется ее разработка. В профессиональном сообществе ценятся международные сертификаты в области защиты информации. При этом в рамках высшего образования в России по программам блока УГСНП 10.00.00 «Информационная безопасность» в настоящий момент не предусмотрена ориентация на профессиональную сертификацию специалистов. Возможно, в ближайшие годы это связь установится через корреляцию образовательных и профессиональных стандартов.

Таким образом, использование системы вендорнезависимой сертификации дополнительно позволит: выстроить систему взаимосвязи с профессиональным сообществом, отвечать на динамичное изменение предметной области, постоянно актуализировать содержание учебных планов, модулей и дисциплин.

Вендорские образовательные курсы с последующей сертификацией спонсируются конкретной организацией, деятельность которой связана с созданием информационных продуктов или средств обеспечения информационной безопасности [112, с.146]. В зависимости от того, где производится то или иное решение по информационной безопасности, различают отечественные образовательные курсы и сертификации и зарубежные.

К популярным на международном рынке (в том числе и в России) международным образовательным программам и сертификациям относятся программы компаний Amazon, Cisco Systems, Microsoft, Oracle и других.

Cisco Systems организует образовательную деятельность через Сетевую академию Cisco, которая на данный момент имеет представительства в 180 странах мира, а число образовательных учреждений-участников увеличилось с 64 в 1997 году до 11 тысяч на данный момент [89].



Курсы Сетевой академии Cisco, посвященные обеспечению информационной безопасности в компьютерных системах и сетях, включают [90]:

1) «Введение в кибербезопасность» (Introduction to Cybersecurity) – начальный уровень, рассчитан на 15 часов.

2) «Основы кибербезопасности» (Cybersecurity Essentials) – средний уровень, курс рассчитан на 30 часов; рассматриваются вопросы киберпреступности и кибербезопасности, принципы конфиденциальности, целостности и доступности; тактика, методы и процедуры, используемые киберпреступниками; технологии, продукты и процедуры, используемые для защиты информации.

3) «Облачная безопасность» (Cloud Security) – средний уровень, курс рассчитан на 35 часов. Ориентирован на сертификацию CCSK (сертификат знаний об облачной безопасности).

4) «Сотрудник КиберОпс» (CyberOps Associate) – средний уровень, курс рассчитан на 70 часов; рассматриваются вопросы раскрытия киберпреступлений, кибершпионажа.

6) «Основы интернета вещей: безопасность интернета вещей» – средний уровень, 50 часов.

7) «Сетевая безопасность» (Network Security) – продвинутый уровень, 70 часов

Образовательные организации США, Великобритании, Германии и Франции активно работают в направлении интеграции реализуемых программ подготовки с вендорскими учебными курсами Сетевой академии Cisco.

Так, ученые британского факультета математики, вычислительной техники и технологий Н. Мосс и Э. Смит сообщают об успехе Открытого университета Соединенного Королевства (UKOU) в реализации учебной программы Cisco Exploration в качестве курса бакалавриата с использованием смешанной модели дистанционного обучения [188]. Университет осуществляет поддержку образовательного процесса по курсу и предоставляет сертифицированного преподавателя (инструктора) для обеспечения высокого качества подготовки.

Учебно-методические материалы для обучения и контроля знаний предоставляются Сетевой академии Cisco. Доступ к онлайн-материалам осуществляется через домашнюю страницу студента. Авторы отмечают, что обучение практическим навыкам обеспечивается использованием реальных сетевых инструментов с удаленным доступом к оборудованию (маршрутизаторам и коммутаторам), при этом эти инструменты не являются симулятором, а позволяют получать доступ к консольному порту реального сетевого оборудования.

Учетные записи в NetLab+ организованы таким образом, чтобы преподаватели могли контролировать работу студентов и проводить занятия по мере необходимости.

Американский исследователь Дж. Мерфи описывает разработанную модель контроля устройств при изучении вендорских курсов Cisco, которая позволяет контролировать сложность заданий и, следовательно, может использоваться в качестве основы для преподавания как вводных, так и углубленных курсов. Эти модели были использованы в качестве педагогической основы для учебных программ бакалавриата и магистратуры по сетевым технологиям, а также для оценки результатов. Прделанная авторами работа свидетельствует о том, что эти модели повышают качество обучения студентов на всех уровнях: то есть, те студенты, которые изучали администрирование компьютерных сетей, но не обучались по этим моделям, набрали меньше баллов на экзаменационном тестировании, чем студенты, обучавшиеся по таким моделям [181, с. 9.134.1; 112, с. 147].

Исследование других авторов (С. Арияпперума, К. Минхас, Политехнический университет Англии, Великобритания) также было посвящено программе по безопасности компьютерных сетей Сетевой академии Cisco. В работе проводится анализ учебной программы с учетом опроса мнений преподавателей и студентов для оценки эффективности интеграции вендорского образовательного курса с конкретными дисциплинами в области информационной безопасности. Данные об использовании вендорских курсов

были собраны с помощью анализа файлов журналов веб-сервера, на котором размещены педагогические документы. В рамках сообщества Сетевой академии Cisco был проведен онлайн-опрос в Европе, на Ближнем Востоке и в Африке. Результаты также показали высокую эффективность предлагаемой учебной программы по сетевой безопасности [123, с. T2C-1].

Образовательные организации Германии уже с 1997 года начали реализовывать образовательные программы по компьютерным сетям под руководством производителя сетевого оборудования в форме партнерства министерств и компании Cisco Systems. М. Лоттер отмечает, что данная образовательная инициатива зарекомендовала себя в профессиональном образовании как высокоэффективная и вносит признанный вклад в повышение готовности к профессиональной деятельности специалистов в области информационных технологий [171, с.70; 112,с. 147]. В контексте профессионального образования, вендорские образовательные курсы с последующей сертификацией рассматриваются в качестве возможности получения дополнительной квалификации, которая значительно увеличивает конкурентоспособность будущего специалиста на рынке труда. Автор акцентирует внимание на том, что профессиональная значимость выпускников возрастает как на национальном, так и на международном уровне.

В университете Реймса (Шампань, Франция) в образовательной программе магистратуры по направлению подготовки «Безопасность и администрирование сетей» также реализуется в условиях интеграции с образовательными ресурсами Сетевой академии Cisco. Обучение ведется в тесном взаимодействии теории и практики. В ходе прохождения лабораторных работ студенты имеют возможность практиковаться с реальным оборудованием (маршрутизатор, коммутатор и беспроводная точка доступа семейства Cisco), что позволяет развивать и администрировать модели компьютерных сетей. Обучающиеся в рамках данного курса работают со сложными сетевыми архитектурами, VPN-туннелями, брандмауэрами и другими программными и аппаратными сервисами обеспечения защиты компьютерных сетей [115, с.161].

Вендорские учебные курсы отечественных ИТ-компаний набирают популярность в системе подготовки специалистов. Например, один из крупнейших отечественных разработчиков программ защиты компьютерных систем, Лаборатория Касперского, предлагает свою многоуровневую систему сертификации специалистов. 1-й уровень KL Certified Professional подтверждает «статус для ИТ-специалистов на знание внедрения, настройки и поддержки различных продуктов Лаборатории Касперского» [72]. 2-й – KL Certified Systems Engineer «предназначен для профессионалов в сфере защиты информации. Статус подтверждает знание процесса внедрения и управления системой защиты любой сложности и размера, основанной на продуктах Лаборатории Касперского» [72]. Следующий – KL Certified Sales Engineer – «это статус для профессионалов, задействованных в предпродажной подготовке, непосредственно в процессе продажи и постпродажной поддержке» [72]. Статус последнего уровня – KL Certified Consultant – «показывает умение спроектировать систему защиты сети на базе продуктов Лаборатории Касперского и внедрить ее» [72].

Также проводится сертификация и по другим отечественным решениям по защите информации, например сертификация технических специалистов и специалистов по продажам по продуктам Dallas Lock. Следует отметить, что программно-аппаратные средства Dallas Lock проходят регулярную сертификацию ФСТЭК РФ и, таким образом, являются доверенным средством защиты информации.

Подобные курсы целесообразно внедрять в рамках таких дисциплин, как «Программно-аппаратная защита информации», «Защита от вредоносных программ», «Защита программ и данных» и других подобных дисциплин. Как правило, компании-разработчики достаточно активно сотрудничают с образовательными организациями, как высшего, так и средне профессионального образования, предоставляя свои продукты по льготным ценам или учебные версии программного обеспечения, обучая преподавателей в рамках курсов и стажировок. Так, еще в 2005 году проводились курсы-стажировки для преподавателей вузов в Лаборатории Касперского [48].

Таким образом, положительный опыт сотрудничества образовательных организаций в США, Великобритании, Германии и Франции с ИТ-компаниями, предоставляющими собственные образовательные курсы и линейки сертификации по выпускаемым информационным продуктам может быть применим и в России. Подобное сотрудничество без сомнения является взаимовыгодным для ИТ-компаний и вузов: *с одной стороны*, вуз имеет возможность получать программные и аппаратные решения крупных вендоров, постоянно актуализировать содержание учебных дисциплин применительно современным реалиям, преподаватели имеют возможность таким образом повышать свою квалификацию; *с другой стороны*, вендоры имеют возможность популяризировать собственные решения по защите информации среди студентов и сотрудников, найти новых клиентов, а также сформировать отложенный спрос к собственным продуктам [112, с.148].

Вместе с тем, мы полагаем, что в связи с отсутствием в настоящее время отечественной системы вендорнезависимой сертификации специалистов по информационной безопасности нецелесообразно использовать международные сертификации в рамках реализации основных образовательных программ блока 10.00.00 «Информационная безопасность» в виду возможных конфронтаций по отечественному и зарубежному нормативному регулированию предметной области и повышенных требований к опыту работы в данной сфере.

## ВЫВОДЫ ПО ГЛАВЕ 1

В первой главе обоснована целесообразность проведения сравнительно-сопоставительного анализа в рамках следующих методологических подходов: *системного* (позволит выявить элементы системы образования в области информационной безопасности, системообразующие факторы и отношения рассматриваемых процессов профессионального образования будущих специалистов по информационной безопасности, а также выявить критерии сопоставления систем профессионального образования будущих специалистов по информационной безопасности); *информационного* (позволит рассмотреть каждую образовательную программу по информационной безопасности в разных странах как информационную модель); *историко-логического* (рассмотрение историко-логической последовательности этапов становления деятельности по защите информации и их взаимосвязь с системой подготовки специалистов, что позволит обнаружить отдельные причинно-следственные связи).

Предложены методика и этапы проведения сравнительного исследования и выбраны следующие методы: анализ информационных ресурсов сети Интернет, системный анализ информационных источников, описательный, сравнительно-сопоставительный, исторический, метод классификации, анкетирование, тестирование, метод самооценки и статистический метод.

Рассмотрены системы профессионального образования специалистов по информационной безопасности в России, США, Великобритании, Германии и Франции.

Отечественная система профессионального образования будущих специалистов по информационной безопасности представлена уровнями среднего профессионального, высшего и дополнительного образования. Профессиональная подготовка будущих специалистов по информационной безопасности в России ориентируется, в большей степени, на техническую и

естественно-научную составляющие. Акцент на техническую сторону, на наш взгляд, обусловлен аспектами исторического развития государственной системы защиты информации. Естественно-научная составляющая обеспечивается изучением программно-аппаратных методов защиты информации, базирующихся на математических основах обеспечения информационной безопасности, алгоритмизации и программирования. В то же время отечественные образовательные программы содержательно включают правовую сторону гуманитарной составляющей информационной безопасности.

Усиленную базовую естественно-научную подготовку (включающую в себя специальные разделы физики, математики, алгоритмизации и программирования) будущих специалистов по информационной безопасности следует рассматривать как положительную черту российского профессионального образования. Кроме того, положительной чертой также является формирование способностей выпускников обеспечивать комплексную безопасность в информационной сфере (практически все отечественные образовательные программы включают разделы, посвященные организационным и правовым, программным и аппаратным, техническим (инженерно-техническим) и криптографическим методам защиты информации).

Образование в сфере защиты информации в Великобритании ориентируется на подготовку кадров, способных обеспечить информационную безопасность прежде всего естественно-научной и гуманитарной составляющей. Вместе с тем практически не уделяется внимание технической составляющей информационной безопасности. Все образовательные программы четко ориентируются на узкий круг вопросов защиты информации в той или иной сфере, и не обуславливают комплексный подход к обеспечению безопасности данных. Выпускники английских программ по информационной безопасности востребованы преимущественно в частных организациях.

Образование в сфере защиты информации в США, как и в Великобритании, ориентируется на подготовку кадров, способных обеспечить информационную безопасность, в большей степени, естественно-научную, а

также гуманитарную составляющие информационной безопасности; при этом технической сфере уделяется мало внимания. Рынок трудоустройства выпускников, прежде всего, находится в бизнес-структурах.

Национальная система профессионального образования в области информационной безопасности в Германии направлена на обучение специалиста, способного решать задачи, прежде всего, гуманитарной составляющей информационной безопасности (превалируют направления подготовки и дисциплины в образовательных программах по правовому обеспечению информационной безопасности, страхованию информации, управлению информационной безопасностью), а также естественно-научной составляющей (криптографическая и программно-аппаратная защита информации). Образование в сфере информационной безопасности в Германии практически не предусматривает решение вопросов технической составляющей. Отмечено, что рынок трудоустройства выпускников, в основном, это бизнес-структуры, в том числе в промышленности, страховании, торговле.

Во Франции содержание всех образовательных программ по информационной безопасности акцентировано на изучение криптографических методов защиты информации и математический цикл образования. Цель профессионального образования в освещаемой области во Франции – это формирование способности решать вопросы естественно-научной и гуманитарной составляющих информационной безопасности. Причем, значительное внимание уделяется естественно-научной составляющей, а именно вопросам криптографии. Выпускник должен решать задачи защиты информации в государственных и в частных структурах. Причем акцентируется внимание на государственном секторе, что имеет общие черты с российским профессиональным образованием по информационной безопасности.

Показано, что американские, британские, немецкие и французские образовательные программы по информационной безопасности зачастую интегрированы с вендорскими образовательными курсами, а также содержательно ориентируются на будущую вендорнезависимую сертификацию выпускников.



В контексте профессионального образования, вендорские образовательные курсы с последующей сертификацией рассматриваются зарубежными авторами как возможность повышения качества обучения студентов на всех уровнях и получения дополнительной квалификации, которая значительно увеличивает конкурентоспособность будущего специалиста на рынке труда. Профессиональная значимость выпускников, имеющих подобные сертификаты, возрастает как на национальном, так и на международном уровне.

Сделан вывод о том, что положительный опыт сотрудничества образовательных организаций с ИТ-компаниями, предоставляющими собственные образовательные курсы и линейки сертификации (вендорские курсы и сертификации) по выпускаемым информационным продуктам может быть применен и в России. Однако в связи с отсутствием в настоящее время отечественной системы вендорнезависимой сертификации специалистов по информационной безопасности нецелесообразно использовать международные сертификации в рамках реализации основных образовательных программ блока 10.00.00 «Информационная безопасность».

## **2 СРАВНИТЕЛЬНО-СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОПЫТНО-ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ИНТЕГРАЦИИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ С ВЕНДОРСКИМ УЧЕБНЫМ КУРСОМ**

### **2.1 Становление системы профессионального образования специалистов по информационной безопасности**

Специфика профессиональной деятельности специалиста по информационной безопасности, так или иначе, должна учитываться при формировании образовательной среды. С этой точки зрения рассмотрим, каким образом оказало влияние отношение к информационной безопасности на государственном уровне на профессиональное образование будущих специалистов по информационной безопасности и защите информации [3, с.58].

В §1.1 при определении методологических подходов диссертационного исследования, было отмечено, что целесообразно рассмотреть специфику становления профессиональной подготовки будущих специалистов по информационной безопасности во взаимосвязи с наиболее важными историческими событиями в рассматриваемом контексте при использовании историко-логического подхода. Подразумевается, что историко-логический подход будет способствовать выявлению базовых закономерностей взаимозависимости отдельных элементов системы профессионального образования специалистов по информационной безопасности и деятельности по формированию государственной системы защиты информации, а также поможет выявить этапы становления отечественной системы профессионального образования специалистов по информационной безопасности [3, с.58].

Вместе с тем очевидно отсутствие синхронизации подобных процессов в разных странах, поэтому мы не пытаемся связать этапы становления профессиональной подготовки будущих специалистов с точной хронологией событий. С другой стороны, информатизация мирового сообщества и однотипные информационные угрозы способны фрагментарно стирать географические и политические границы, формируя тенденцию к синхронизации отдельных событий. Тем не менее, мы полагаем, что историко-логический анализ приведет нас к выводу, что становление отдельных элементов системы профессиональной подготовки будущих специалистов по информационной безопасности формируются под влиянием государственной системы защиты информации [3, с.58].

Решая подзадачу выделения этапов развития профессионального образования специалистов по информационной безопасности, необходимо проанализировать литературные источники по периодизации становления государственных систем защиты информации в России и зарубежных странах. В отечественной литературе нами было обнаружено несколько подходов к периодизации деятельности по защите информации авторов: В.И. Аверченков [1], В.Н. Лопатин [52], А.А. Малюк [56].

Беря за основу этапы развития носителей информации, В.И. Аверченков выделяет три периода [1, с.10]:

I этап связан с появлением письменности и возможности фиксировать информацию на твердом носителе и, как следствие, появляется необходимость скрывать записанную информацию, что обуславливает развитие первых методов защиты информации: стеганографии и криптографии.

II этап связан с появлением с середины 1930 гг. технических средств хранения и передачи информации, в связи с чем, появилась потребность защиты информации по техническим каналам инженерно-техническими методами.

III этап связан с изобретением первых ЭВМ в середине XX века. Современный этап автор дополнительно подразделяет на три периода: *начальный* (60-е – 70-е гг.), когда под процессом защиты информации подразумевалось

предупреждение несанкционированного доступа, *период развития* (70-е – 80-е гг.), для которого характерен поиск и совершенствование новых методов и средств защиты информации, и *современный этап* (80-е гг. – по настоящее время), когда к защите информации стали применять научный подход, формируя научно-методологический базис решения проблемы [1, с.10].

В то же время В.Н. Лопатин выделяет семь этапов формирования системы информационной безопасности [52].

I-й этап (до 1816 г.) «характеризуется использованием естественно возникших средств информационных коммуникаций». Мы полагаем, что под такими технологиями ученый, как и В.И. Аверченков, подразумевает развитие письменности. Однако при характеристике деятельности по обеспечению безопасности данных на данном этапе не говорится о развитии шифрования. Данный этап рассматривается с точки зрения организационных мер.

II-й этап (с 1816 г.), аналогично второму этапу, выделяемому В.И. Аверченковым, связан с появлением технических средств передачи информации, что определило становление средств защиты данных по техническим каналам связи.

III-й этап (с 1935 г.) характеризуется использованием «активных маскирующих и пассивных имитирующих радиоэлектронных помех» и, как следствие, изобретением радиолокационных и гидроакустических средств.

IV-й этап (с 1946 года) характеризуется появлением первых ЭВМ. Однако автор отмечает, что изначально с целью защиты оборудования использовались только методы физического ограничения доступа.

V-й этап (с 1965 года) связан появлением компьютерных сетей, при этом, как и прежде, в основном применялись методы физической защиты с помощью разграничения доступа к ресурсам.

VI-й и VII-й этапы (с 1973 года) были связаны с увеличением мобильности устройств, появлением глобальной сети Интернет и спутниковой связи, когда угрозы информационного характера усугубились и масштабировались, появилась необходимость в разработке критериев и стандартов безопасности.

Анализируя два подхода к периодизации деятельности по защите информации, приходим к выводу, что I-й этап ученые выделяют примерно одинаково, и связан он с развитием письменности. Как отмечалось выше, В.И. Аверченков I-й этап характеризует становлением методов стеганографии и криптографии, а В.Н. Лопатин связывает данный период с организационным обеспечением личной информационной безопасности человека или сообщества.

По временному периоду II-й и III-й этап В.Н. Лопатина совпадает со II-м этапом, выделяемым В.И. Аверченковым и, в обоих случаях, характеризуются развитием инженерно-технических методов защиты информации.

III-й этап В.И. Аверченкова по временным рамкам совпадает с IV-VII этапами В.Н. Лопатина и обусловлен появлением и развитием компьютеров. При этом IV-ый и V-ый этапы В.Н. Лопатин (в эпоху первых ЭВМ) связывает, прежде всего, с применением «методов и способов ограничения физического доступа к оборудованию». Началом V-го этапа, который обусловлен появлением информационно-коммуникационных сетей, ученый выделяет 1965 год. На наш взгляд, это невозможно, так как первая компьютерная сеть ARPANET (прообраз глобальной сети Интернет) была создана Министерством обороны США позже, в 1969 году.

Обобщение иностранных источников показывает, что зарубежные исследователи считают, что деятельность по обеспечению безопасности данных началась с изобретения первых компьютеров и все вопросы по защите информации касаются только защиты компьютерных систем и сетей. Майк Линетт (США) [178] I-м этапом обеспечения информационной безопасности выделяет появление первых принципов программно-аппаратного разграничения доступа к ЭВМ, а также разработкой и применением первых средств идентификации и аутентификации пользователей в 60-х гг.

Следующий II-й этап характеризуется появлением первых отдельных компьютерных преступлений, связанных с нарушением конфиденциальности и целостности информации и развитием использования компьютерных сетей в 70-х гг.

На III-м этапе начинают развиваться методы правовой защиты информации, так как преступления, совершенные с использованием компьютерных систем и сетей, приобретают массовый характер и государство активизирует борьбу с киберпреступностью.

IV-й этап (90-е гг.) характеризуется появлением глобальной сети Интернет, когда информатизация западного общества стала заметно повышаться, а злоумышленники увидели в этом потенциальный источник дохода. В ответ на новые угрозы появились первые межсетевые экраны и антивирусные программы, которые помогали защититься в интенсивно растущем глобальном пространстве.

V-й этап (00-е гг.) связан с осознанием правительством опасности хакерских атак и значительным отягощением наказания за компьютерные правонарушения.

И последний, VI-й этап (10-е гг.), когда стал получать значительное распространение комплексный подход к обеспечению компьютерной безопасности, теперь используются все методы и средства защиты информации. Организации внедряют комплексные меры информационной безопасности, которые предотвращают ошибки среди своих сотрудников, тем самым делают данные недоступными для злоумышленников.

В основе периодизации другого исследователя и эксперта, Теда Джулиана лежит эволюция мер и средств защиты информации от вредоносного программного обеспечения [195]. Всего Тед Джулиан выделяет четыре этапа:

I этап (80-е – начало 90-х гг.) – появление первых деструктивных программ, так называемых «компьютерных червей», что послужило толчком к реализации нового для того времени вида угрозы – DoS-атаки. На что профессиональное сообщество отреагировало созданием первых антивирусных программ и написанием первых стандартов защиты информации.

II этап (90-е гг.) – характеризуется усилением роста реализованных атак с использованием вредоносного программного обеспечения, когда отмечается качественное развитие методов и технологий защиты от вирусов.

III этап (конец 00-х гг.) – атаки на компьютерные системы стали более масштабными и нацеленными, их основным объектом становятся платежные

системы, а системы защиты информации, отвечая на актуальные угрозы, стали усложняться и, при проектировании методов защиты, начал применяться комплексный подход.

IV этап (настоящее время) – характеризуется одновременным усложнением технологий и методик защиты информационных систем, технологий и методик, используемых киберзлоумышленниками. Вместе с тем вопросы обеспечения информационной безопасности приобрели критически важное значение в обществе [3, с.59].

Анализ описанных и иных [122, 138, 145] примеров периодизации становления систем защиты информации приводят нас к выводу, что зарубежный (в первую очередь – американский) подход подразумевает под информационной безопасностью и защитой информации исключительно программно-аппаратную защиту компьютерных систем и сетей. В отличие от западных коллег, российские исследователи отдельно выделяют ранние «докомпьютерные» методы защиты информации [3, с.59].

За рабочую версию примем периодизацию В.И. Аверченкова, исходя из понятности выделенного принципа разделения на этапы (эволюция видов носителей информации). Однако для более детального рассмотрения III-го, «компьютерного» периода целесообразно дополнительно использовать подходы зарубежных авторов.

Как было отмечено выше, профессиональное образование будущих специалистов по информационной безопасности, целесообразно рассмотреть внутри формирующейся и перманентно трансформирующейся профессиональной среды, включающей в себя государственную систему защиты информации, технологии и средства обеспечения безопасности данных, саму информацию, подвергающуюся защите. Предполагается, что попытка периодизации становления отечественного профессионального образования специалистов по защите информации поможет подробнее проанализировать предметную область историко-логического анализа в контексте наиболее важных событий, повлиявших на формирование системы безопасности в информационной сфере,

что, в свою очередь, зависит от появления и нарастания новых угроз безопасности [3, с.59].

С целью выделения этапов профессионального образования специалистов по информационной безопасности нами были ретроспективно проанализированы перечни отечественных специальностей и направлений подготовки, стандарты второго и третьего поколений, по которым велась подготовка в последние десятилетия, а также научные источники по теме исследования. Таким образом, было выделено пять этапов, подробно представленных в статье [3, с.59].

Мы полагаем, что первые два этапа ориентировочно совпадают с профессиональным образованием зарубежных специалистов, так как общество получало сопоставимое развитие в информационной сфере. А во второй половине XX века западное профессиональное образование будущих специалистов стала заметно опережать российское вследствие динамично развивающейся информатизации, «прорывного» развития в сфере компьютерных систем и сетей, завоевания позиции мирового лидера в ИТ-сфере [3, с.59-61].

***Этап I. Подготовка кадров, способных решать фрагментарные вопросы защиты информации в «закрытых» ведомственных учреждениях (до 40-х гг.).***

С появлением и развитием криптографических методов защиты информации и использованием их в государственных целях стала появляться необходимость в передаче этих специализированных знаний. По мере развития государственной системы безопасности, так или иначе, частью которой всегда была информационная сфера, стала задача по обучению кадров, способных обеспечить сокрытие передаваемой информации и, в то же время, проводить криптоанализ зашифрованных сообщений противника. Таким образом, мы полагаем, в этот период зарождались первые элементы системы профессионального образования специалистов по защите информации в рамках подготовки кадров, способных решать отдельные вопросы защиты информации при специальных государственных службах, актуальных в то время [3, с.61].

***Этап II. Подготовка специалистов по информационной безопасности в учреждениях высшего образования по «закрытым» программам (1940-е –***



*1984 г.*). Для данного периода времени характерно, с одной стороны, глобальное политическое событие, связанное с информационным противоборством биполярного мира – так называемая «холодная война», и революционное техническое открытие с другой стороны – изобретение ЭВМ Джоном фон Нейманом и его коллегами, которые сформулировали первые принципы архитектуры компьютеров (1945 г.) [3, с.61, 168] и дальнейшее их развитие, а также появление первых вычислительных сетей.

Вычислительные сети, связывающие несколько ЭВМ в США, появились чуть более чем через 20 лет – в 1969 году. Задачей сетей изначально становилось обеспечение надежного канала передачи информации для Министерства обороны США. Первая компьютерная сеть представляла собой соединение двух терминалов Калифорнийского и Стэнфордского университетов и имела название сеть ARPANET – прообраз современной сети Интернет. В статье Ю.А. Савостицкого «История развития глобальных компьютерных сетей» отмечается, что отечественные вычислительные сети появились и развивались с отставанием от западных разработок в десятилетие [87, с.61]. В дальнейшем такое отставание сократилось в связи с тем, что с распадом СССР интенсивно начали внедряться и активно использоваться западные технологии и расширился информационный обмен с зарубежными странами.

Ввиду информационной «закрытости» зарубежных программ в области защиты информации в этот период нам не удалось проследить эволюцию рассматриваемых образовательных программ в зарубежных странах. Однако мы полагаем, что «скачок» в информационных технологиях и мировое информационное противоборство стимулировали интенсивное развитие профессионального образования специалистов по защите информации и за рубежом.

В нашей стране в данный период появилась первая отечественная «закрытая» образовательная программа по криптографии (1949 год) на базе закрытого отделения Московского государственного университета имени М.В. Ломоносова (МГУ) совместно с Высшей школой Комитета государственной

безопасности СССР. Позже эти программы расширились за счет внедрения отдельных тем и дисциплин по программным и аппаратным методам защиты информации [76].

***Этап III. Появление отдельных «открытых» образовательных программ по информационной безопасности в учреждениях высшего образования (1985 – конец 1990-х гг.).*** Для данного периода времени характерно начало сотрудничества между ранее противоборствующими странами СССР (Россией) и США, в том числе сотрудничество осуществляется и в информационной сфере, начинается массовая информатизация всех государственных и общественных сфер. Отечественные ученые отмечают, что именно в этот период отечественные вузы начали реализовывать «открытые образовательные программы» в сфере защиты информации [76, с.19].

В 1994 году были выделены три специальности по информационной безопасности: по защите телекоммуникационных систем (блок 200000), а также по организации и технологии защиты информации и по комплексному обеспечению информационной безопасности (блок 220000) [68], а в 1995 году дополнены специальностью «Криптография», входящей в блок естественно-научных специальностей (010000) [66; 76, с.19].

В течение следующих лет были законодательно утверждены содержание подготовки и требования к выпускникам, когда были приняты первые стандарты профессионального образования в области защиты информации (ГОС ВПО).

В этот же период было сформировано учебно-методическое объединение по информационной безопасности, задачей которого стала координация деятельности образовательных организаций разных уровней (среднего профессионального, высшего, дополнительного), реализующих образовательные программы по информационной безопасности.

Таким образом, в 90-е гг. (что соответствует выделенному нами III-у этапу) характерно значительное повышение интереса к сфере защиты информации и обеспечению информационной безопасности, когда вслед за появлением отдельных «открытых» образовательных программ по информационной

безопасности в учреждениях высшего образования стали утверждаться первые образовательные стандарты по специальностям в сфере информационной безопасности, сформировалось УМО по информационной безопасности – все это дало толчок активному развитию и становлению профессионального образования в области защиты информации в России.

Вместе с тем, обращаясь к трудам С.Н. Гриняева [31, 32], следует обратить внимание на то, что, несмотря на повышенный интерес к вопросам защиты информации в рассматриваемый период, все же информатизация общества и объем используемых средств ИКТ нарастал интенсивнее индустрии средств обеспечения информационной безопасности и новых разработанных технологий защиты информации. Прежде всего они становились ответом на уже имеющиеся распространенные и принесшие тот или иной ущерб информационные угрозы. Системы защиты информации, создаваемые в этот период, не были рассчитаны на только зарождающийся кибертерроризм в мировом информационном пространстве, а сами «системы и не рассчитывались на функционирование в условиях воздействия поражающих факторов хакеров-террористов» [32, с.190].

Мы полагаем, что, с одной стороны, интенсивное развитие средств защиты информации и повышенный интерес к вопросам обеспечения информационной безопасности, а с другой стороны, отставание технологий защиты от реальных темпов информатизации дало стимул к качественной трансформации системы профессионального образования специалистов по информационной безопасности и переходу к массовой реализации образовательных программ по информационной безопасности в образовательных организациях.

#### ***IV этап. Начало массовой реализации программ по информационной безопасности в образовательных учреждениях разного уровня (2000–2010 гг.).***

В ответ на вновь появившиеся угрозы международного терроризма, в том числе в информационной сфере и с использованием информационных технологий, происходит значительный «прорыв» к пониманию проблем информационной безопасности на государственном и общественном уровнях. События, произошедшие 11 сентября 2001 года в США, стали «точкой отсчета не только

для целого ряда специальных служб и правоохранительных органов, но и для разработчиков информационных систем и производителей средств защиты информации» [32, с.190].

В 00-е годы XXI столетия происходит трансформация взглядов на потребителя средств защиты информации: ранее считалось, что специалисты в данной области требуются, в основном, только в государственных структурах, в которых циркулирует конфиденциальная информация или государственная тайна. С данного периода любая организация, независимо от формы собственности, нуждалась в компетентном специалисте, имеющем профильное образование, для обеспечения целостности, доступности и конфиденциальности информации и информационных систем. Так, закон «О персональных данных», принятый в 2006 году фактически обязывает все организации, хранящие и обрабатывающие персональные данные сотрудников, иметь в штате специалиста по защите информации (или, как минимум, ИТ-специалиста, прошедшего курсы повышения квалификации или курсы переподготовки по информационной безопасности). Повышение спроса на квалифицированных специалистов, способных обеспечить безопасность информации, в том числе, в частных бизнес-структурах, сформировало социальный заказ для образовательных организаций.

В 2000 году перечень образовательных программ по информационной безопасности был расширен и данные программы впервые были выделены в отдельный блок специальностей «Специальности в области информационной безопасности» [69], приняты новые образовательные стандарты. В 2002 году была создана еще одна специальность – по противодействию техническим разведкам [3, с.63].

Заметим, что до настоящего времени две специальности (по криптографии и по противодействию техническим разведкам), носят конфиденциальный характер, не являются общедоступными и не реализуются «гражданскими» образовательными организациями.

В 2005 году, без изменений самих специальностей и образовательных стандартов по ним, блок специальностей поменял свое название вместе с шифрами: 090000 «Информационная безопасность» [71].

С 2002-2003 учебного года организации высшего образования по всей России начали реализовывать образовательные программы по новым специальностям в области информационной безопасности. Спустя 2 года, общая численность таких вузов превышала сотню. Вместе с тем, как отмечают А.П. Коваленко и Е.Б. Белов, к середине 00-х гг. XXI века были разработаны «...примерные учебные планы и примерные программы дисциплин...» и другие учебно-методические материалы [44, с.125].

В то же время, В.П. Шерстюк, разделяя два направления подготовки будущих специалистов по информационной безопасности: технологическое и гуманитарное, отмечает, что «...технологическая составляющая информационной безопасности разработана более тщательно и глубоко, в то время как гуманитарная составляющая – гораздо слабее», и задает вектор будущих исследований: «...развитие гуманитарной составляющей системы обеспечения информационной безопасности должно сегодня стать приоритетным направлением приложения наших усилий» [117, с.38]. В том числе, исходя из обозначенного, нами выделен следующий этап.

*У этап. Подготовка специалистов по информационной безопасности по сферам деятельности (с 2010 г. по настоящее время).* На данном этапе происходит формирование научных методов защиты информации и базиса обеспечения безопасности информации в гуманитарной составляющей [3, с.63]

В 2009-2011 гг. были приняты новые образовательные стандарты высшего профессионального образования по направлениям подготовки бакалавриата, специалитета, магистратуры. Появились два новых направления подготовки, характерные для обеспечения безопасности данных по отраслям, одна из них – в экономической сфере, в банковских структурах, другая – в правоохранительной сфере. Вероятно, прослеживается намеченная тенденция к профилизации

технологий обеспечения информационной безопасности по сферам деятельности [3, с.64].

Таким образом, анализ становления отечественного и зарубежного профессионального образования по защите информации в рамках историко-логического подхода были определены следующие этапы развития:

- этап подготовки кадров, способных решать фрагментарные вопросы защиты информации в «закрытых» государственных организациях (до 1940х гг.);
- этап подготовки специалистов по информационной безопасности в учреждениях высшего образования по «закрытым» программам (1940-е-1984 гг.);
- этап появления отдельных «открытых» образовательных программ по информационной безопасности в учреждениях высшего образования (1985-конец 1990-х гг.);
- этап массовой реализации программ по информационной безопасности в образовательных учреждениях разного уровня (2000-2010 гг.);
- этап подготовки специалистов по информационной безопасности по сферам деятельности (с 2010 г. по настоящее время).

Определенные этапы становления профессионального образования по защите информации, анализируются на фоне эволюции сферы информационно-коммуникационных технологий, а также методов и средств обеспечения безопасности данных.

В статье, посвященной данному этапу диссертационного исследования [3], нами были проанализированы некоторые исторические аспекты становления систем обеспечения безопасности данных в зарубежных государствах и их воздействие на развитие системы профессиональной подготовки специалистов по защите информации через призму отношения зарубежных стран к таким понятиям, как «информационная война» и «информационное противоборство» [31, 32, 57, 78]. Были обнаружены некоторые соответствия в становлении государственных систем обеспечения безопасности информации и содержательной компонентой в современном профессиональном образовании специалистов. Так, выделены высокая популярность программ обучения по

расследованию цифровых преступлений в США, «усиленный» блок юридических дисциплин в Великобритании, нацеленность на изучение криптографических методов защиты информации во Франции и другие [3, с.60-61].

## 2.2 Общие черты и ключевые различия в компонентах подготовки будущих специалистов по информационной безопасности в России и за рубежом

Анализ национальных систем профессионального образования будущих специалистов по информационной безопасности, проведенный в 1-ой главе, показал, что эти системы имеют существенные различия. Поэтому в нашем исследовании целесообразнее использовать сопоставление систем подготовки: «сопоставление проводится для систем, которые не имеют достаточного количества общих существенных оснований для сравнения, то есть базируются на разных культурных традициях» [94, с.30].

Одной из основных задач сравнительно-сопоставительного анализа подготовки будущих специалистов по информационной безопасности является выявление критериев сопоставления. Для поиска критериев сопоставления различных систем профессионального образования специалистов по информационной безопасности нами был применен *системный подход*, с точки зрения которого важно выявить элементы системы образования специалистов по защите информации, системообразующие факторы и отношения рассматриваемых процессов подготовки будущих специалистов.

Профессор А.Н. Джуринский под системой высшего образования понимает «совокупность вузов, структуру, содержание и организацию учебного процесса» [34, с.7]. В докторской диссертации И.Р. Луговская указывает на важность параметрического подхода к анализу систем школьного образования разных стран, когда необходимо учитывать совокупность параметров для анализа систем образования разных стран, среди которых и структурные элементы образовательной системы, и ее интегральные признаки [53, с. 11].

Вместе с тем, принимая во внимание данные подходы, мы, рассматривая образовательную систему, также опирались на мнения ряда авторов [42; 104, с.14] относительно разделения на подсистемы: содержательную, функциональную и организационно-управленческую.



«Содержательная подсистема отражает суть образования, а также конкретное содержание образования того или иного уровня» [104, с.14]. С точки зрения сравнительно-сопоставительного анализа нам представляется важным рассмотреть следующие элементы содержательной подсистемы: содержание образовательных стандартов (при наличии), направления подготовки (профили, специализации), по которым реализуются образовательные программы в разных странах, а также непосредственно содержание образовательных программ (дисциплины, модули, практики, направления научно-исследовательских работ, и другое).

Функциональная подсистема включает в себя, прежде всего, образовательные организации, которые реализуют соответствующие образовательные программы, их структуру, кадры, сложившиеся формы и методы работы. Так, критериями сопоставления, являющимися элементами функциональной подсистемы стали: образовательные организации, образовательные технологии, профессорско-преподавательский состав, целевая аудитория.

Организационно-управленческая подсистема включает в себя государственные органы, регулирующие вопросы образования и осуществляющие контроль деятельности образовательных организаций. Для проведения сравнительно-сопоставительного анализа элементов организационно-управленческой подсистемы нами выделены критерии, которые, так или иначе, регулируются органами государственного управления в разных странах: сложившиеся ступени подготовки (образовательные маршруты), управление содержанием образовательных программ.

Цель подготовки будущих специалистов по информационной безопасности является системообразующим фактором образовательной системы.

На рисунке 17 представлены выделенные критерии сопоставления педагогических систем профессионального образования.



Рисунок 17 – Критерии сопоставления педагогических систем профессионального образования будущих специалистов по информационной безопасности.

1-й критерий сопоставления педагогических систем – *цель подготовки будущих специалистов по информационной безопасности*. При этом будем формулировать цели обучения специалистов через предметную область профессиональной деятельности выпускников, которые, как показано в первой главе, можно разделить на три составляющие информационной безопасности: естественно-научную, гуманитарную и техническую. Как показал анализ, в каждой стране выделяется в большей степени та или иная составляющая. Также в рамках этого критерия будем рассматривать рынок трудоустройства выпускников: частные (бизнес, промышленность, торговля, страхование и т.п.) или государственные организации.

Далее, необходимо провести сопоставление по перечню *направлений подготовки (профилей, специальностей)*. Профессиональное образование специалистов по информационной безопасности в каждой стране характеризуется, прежде всего, теми направлениями подготовки, по которым ведется обучение. Формируя образовательные программы по этим направлениям

подготовки, образовательные организации, по сути, удовлетворяют социальный заказ государства и общества. Причем, в странах с большим количеством разнообразных программ (США и Великобритания) имеет смысл проводить сравнительно-сопоставительный анализ по выделенным укрупненным блокам направлений подготовки.

Отдельно следует провести анализ и выявить ключевые различия в *содержании образовательных программ* в сфере информационной безопасности. Это позволит сформулировать направления развития отечественной системы профессионального образования по содержательной линии.

Еще один критерий – *образовательные организации* (номенклатура образовательных учреждений по направлению «Информационная безопасность»), в рамках которого необходимо обнаружить и проанализировать колледжи и университеты, реализующие образовательные программы по обеспечению безопасности данных и защиты информации. Внимание акцентируется на том, что анализ проводится только по «гражданским» вузам, имеющим «открытые» образовательные программы по информационной безопасности.

Нам представляется важным провести сравнительный анализ по формам и методам обучения, формам контроля знаний, видам учебных и производственных практик и видам итоговых аттестаций и др. Таким образом, необходимо выделить следующий критерий сопоставления – *образовательные технологии*.

Потенциал любой образовательной программы заключается, прежде всего, в преподавательском составе. Как показывает анализ зарубежных и отечественных образовательных программ, преподавательскую деятельность ведут не только штатные сотрудники, но и приглашенные сторонние специалисты. Это обусловлено тем, что изменение среды, в которой предстоит работать будущим выпускникам, происходит настолько быстро, что привлечение преподавателей со стороны внешних организаций становится просто необходимым. Таким образом, следующим критерием сопоставления выделяем *преподавательский состав, привлекаемый к реализации образовательных программ по информационной безопасности*.

Следующий критерий для анализа – *управление содержанием образовательных стандартов*. Прежде всего, необходимо определить, существуют ли в зарубежных странах государственные образовательные стандарты в области информационной безопасности. На каком уровне осуществляется формирование образовательных стандартов, регламентирующих перечень направлений подготовки, содержание образовательных программ, вариативные и инвариантные дисциплины, количество часов, формы и методы обучения и другое.

Ориентация на Болонский процесс предусматривает переход на двухуровневую модель образования бакалавр-магистр. Важно рассмотреть, какие образовательные маршруты характерны для профессионального образования по информационной безопасности. Поэтому выделен следующий критерий сопоставления – *сложившиеся ступени подготовки будущих специалистов*.

Кроме того, полезно рассмотреть необходимый уровень образования абитуриента, желающего получить образование в области информационной безопасности, что обуславливает выделение критерия – *целевая аудитория*.

Перейдем к сравнительно-сопоставительному анализу систем профессионального образования специалистов по информационной безопасности по выделенным критериям. Для проведения такого анализа будет удобно представить информацию в табличном виде (таблица 1).

На основе данных, приведенных в главе 1 и таблице 1, рассмотрим общие черты и ключевые различия в подготовке специалистов по информационной безопасности в России, Великобритании, Германии, Франции и США.

Таблица 1 – Сопоставление систем профессионального образования будущих специалистов по информационной безопасности в России и за рубежом

Критерий сопоставления	РФ	США	Франция	Германия	Великобритания
<b>Цель подготовки будущих специалистов</b>	Формирование у выпускников способности решения задач обеспечения информационной безопасности с естественно-научной, технической и юридической стороны гуманитарной составляющей информационной безопасности; большое внимание уделяется вопросам обеспечения безопасности данных в государственных организациях	Формирование у выпускников способности обеспечения безопасности данных, прежде всего естественно-научной и гуманитарной составляющей; рынок трудоустройства выпускников преимущественно частные организации	Формирование у выпускников способности решения вопросов естественно-научной и гуманитарной составляющей информационной безопасности, причем, значительное внимание уделяется естественно-научной составляющей, а именно вопросам криптографии; акцентируется внимание на обеспечении безопасности в государственном секторе	Формирование у выпускников способности решения задач, прежде всего, гуманитарной составляющей, а также естественно-научной составляющей информационной безопасности; рынок трудоустройства выпускников-специалистов по защите информации, в основном, бизнес-структуры	Формирование у выпускников способности обеспечения безопасности данных, прежде всего естественно-научной и гуманитарной составляющих информационной безопасности; выпускники востребованы преимущественно в частных организациях
<b>Управление содержанием образовательных программ</b>	Частично формируются под влиянием ФГОС ВО	Устанавливаются образовательной организацией	Устанавливаются образовательной организацией	Устанавливаются образовательной организацией	Устанавливаются образовательной организацией

## Продолжение Таблицы 1

Критерий сопоставления	РФ	США	Франция	Германия	Великобритания
<b>Сложившиеся ступени подготовки будущих специалистов</b>	Среднее профессиональное; высшее (специалитет, бакалавриат, магистратура) очно, очно-заочно; курсы повышения квалификации и переподготовки (с последующей сертификаций, в том числе международной)	Ассоциат; бакалавр, магистр – очно; бакалавр, магистр – дистанционное; курсы (сертификация, в том числе международная)	Профессиональная лицензия в рамках «длинного» цикла, магистр – очно; курсы (сертификация, в том числе международная)	Бакалавр, магистр – очно; курсы (сертификация, в том числе международная)	Бакалавр – три года (полный день), более 3-х лет (неполный день); бакалавр с отличием – четыре года (при полном дне, 4-й год - практика); магистр – один-два года (полный день), три года (неполный день); курсы (сертификация, в том числе международная)
<b>Образовательные организации</b>	Некоторые вузы: ФГАОУ ВО НИЯУ «Московский инженерно-физический институт» ФГАОУ ВО НИУ «Высшая школа экономики» ФГБОУ ВО «ЧГУ им. И.Н. Ульянова» ФГАОУ ВО «БФУ им. И. Канта» ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»	Некоторые вузы - Университет Стайер - Технический университет Колорадо - Международный университет Джонс - Университет Липерпуль - Университет Старфорд - Университет Питсбург - Нью-Йоркский Институт технологий	Некоторые вузы: - Высшая школа Телеком Британь; - Университет в городе Бордо; - Университет в городе Ренн.	Некоторые вузы: - Ганноверский университет имени Лейбница; - Университет в городе Ален; - Боннский университет	Некоторые вузы: - Университет Монфорта; - Университет Хэффлэлла Халлама; - Университет Восточного Лондона; -- Лондонский Университет Метрополитен; - Университет Гламоргана; - Университет Миддлсекса

Продолжение Таблицы 1

Критерий сопоставления	РФ	США	Франция	Германия	Великобритания
<b>Образовательные технологии</b>	<ul style="list-style-type: none"> <li>- Лекции, лабораторные и практические занятия, семинары;</li> <li>- промежуточная аттестация – экзамен, зачет;</li> <li>- прохождение учебной и производственных практик;</li> <li>- выполнение контрольных и курсовых работ;</li> <li>- в отдельных организациях – рейтинго-модульная система обучения;</li> <li>- выполнение и защита ВКР на последнем курсе обучения.</li> </ul>	<ul style="list-style-type: none"> <li>- Лекции, лабораторные занятия, семинары;</li> <li>- промежуточная аттестация – экзамен с получением баллов по кредитной системе оценивания;</li> <li>- практика.</li> <li>- стажировки в промышленности, частных или бизнес-структурах;</li> <li>- выполнение и защита исследовательского проекта (диссертации) в конце обучения</li> </ul>	<ul style="list-style-type: none"> <li>- Лекции, лабораторные занятия, семинары;</li> <li>- акцент на самостоятельную работу и работу в малых группах;</li> <li>- промежуточная аттестация – экзамен с получением баллов по единой системе учета зачетных единиц (ECTS);</li> <li>- стажировки на предприятиях и научно-исследовательских лабораториях;</li> <li>- выполнение и защита исследовательского проекта (диссертации) в конце обучения</li> </ul>	<ul style="list-style-type: none"> <li>- Лекции, лабораторные занятия, семинары;</li> <li>- большинство дисциплин предлагается на выбор;</li> <li>- работа в группах в лабораториях;</li> <li>- промежуточная аттестация в виде письменного экзамена, отчета по самостоятельной работе или по проекту с получением баллов по единой системе учета зачетных единиц (ECTS);</li> <li>- стажировки в ИТ-компаниях;</li> <li>- выполнение и защита исследовательского проекта (диссертации) в конце обучения</li> </ul>	<ul style="list-style-type: none"> <li>- Лекции, лабораторные занятия, исследовательские семинары;</li> <li>- промежуточная аттестация в виде письменного экзамена, отчета по самостоятельной работе или по проекту с получением баллов по единой системе учета зачетных единиц (ECTS);</li> <li>- широкое использование средств сети Интернет для дистанционного обучения (онлайн чаты, видео-курсы, доски объявлений);</li> <li>- стажировки на предприятиях;</li> <li>- выполнение и защита исследовательского проекта (диссертации) в конце обучения</li> </ul>

Продолжение Таблицы 1

Критерий сопоставления	РФ	США	Франция	Германия	Великобритания
<b>Целевая аудитория</b>	Для поступления и обучения с последующим получением квалификации специалиста и бакалавра необходимо иметь аттестат о полном среднем образовании; для поступления в магистратуру необходимо иметь квалификацию специалиста или бакалавра; для поступления в аспирантуру необходимо иметь квалификацию специалиста или магистра	Для поступления и обучения с последующим получением степени ассоциата или бакалавра – необходим диплом о среднем (школьном) образовании; для поступления в магистратуру - при наличии степени бакалавра по близким направлениям подготовки	Для обучения с последующим получением профессиональной лицензии – необходима степень бакалавра (полное среднее образование); для поступления в магистратуру – необходима профессиональная лицензия в сфере компьютерных наук или математики	Для получения высшего образования (бакалавриат) – необходимо иметь среднее образование второй ступени (школьное образование, 13 лет); для поступления в магистратуру – необходимо иметь степень бакалавра в сфере компьютерных наук	Для получения высшего образования необходимо иметь сертификата о полном среднем образовании; для поступления в магистратуру – необходимо иметь степень бакалавра в сфере компьютерных наук



Продолжение Таблицы 1

Критерий сопоставления	РФ	США	Франция	Германия	Великобритания
<b>Профессорско-преподавательский состав и специалисты, осуществляющие подготовку в области информационной безопасности</b>	Научно-педагогические кадры, имеющие базовое образование, а также имеющие ученую степень, соответствующие профилю преподаваемой дисциплины	Научно-педагогические кадры, имеющие степень доктора философии или магистра, приглашенные эксперты	Научно-педагогические кадры, имеющие степень доктора философии или магистра, приглашенные эксперты	Научно-педагогические кадры, имеющие степень доктора философии или магистра, приглашенные эксперты	Научно-педагогические кадры, имеющие степень доктора философии или ведущие специалисты

Педагог С.Н. Широбоков отмечает, что во многих работах по сравнительной педагогике выявление общих черт и ключевых различий в образовательных системах являются основой для теоретического описания развития сравнительного образования [118, с.66]. Вначале остановимся на **общих чертах** в профессиональном образовании специалистов в области информационной безопасности. В каждой стране обобщено профессиональная подготовка будущих специалистов по информационной безопасности имеет для всех стран схожую цель – формирование у будущих выпускников компетенций, необходимых для квалифицированного решения задач обеспечения информационной безопасности в условиях существования угроз [8, с.116].

Профессиональное образование будущих специалистов по информационной безопасности осуществляется в образовательных организациях среднего, высшего и дополнительного образования (с учетом специфики общей системы профессиональной подготовки в каждой рассматриваемой стране). Отдельно стоит заметить, что значительную роль в профессиональном образовании будущих специалистов по информационной безопасности и в России, и в зарубежных странах, играют курсы в рамках дополнительного образования. При этом зачастую зарубежная подготовка ориентируется на дополнительную профессиональную сертификацию своих обучающихся или выпускников по международным стандартам [8, с.116].

Во всех рассматриваемых странах к процессу подготовки привлекаются научно-педагогические кадры, имеющие ученую степень, базовое высшее образование, а также ведущие специалисты со стороны профессионального сообщества.

Анализ систем профессионального образования в рассмотренных зарубежных странах показывает, что они ориентируется на сопоставимость систем профессионального образования, в том числе будущих специалистов по информационной безопасности (применение кредитных систем и распространенного использования системы международной профессиональной

сертификации). Но, при этом, существуют и национальные особенности, которые наиболее ярко выражены во Франции (короткий и длинный циклы обучения, собственная система академических степеней) и Германии (принцип академической свободы). Вместе с тем, данная схожая черта относительно рассмотрения зарубежных программ, является особенной при сопоставлении с российской системой.

Далее перейдем к выделению ряда **ключевых различий** в профессиональном образовании будущих специалистов по информационной безопасности. Рассмотрение ключевых различий проведем по подсистемам, по которым выделялись критерии сопоставления (рисунок 17).

По организационно-управленческой подсистеме были выделены ключевые различия по управлению содержанием образовательных программ и по ступеням подготовки.

Различие в управлении содержанием образовательных программ заключается, прежде всего, в частичном управлении содержанием и требований к выпускникам профильными министерствами, а также органами государственной власти, регулируемыми вопросы защиты информации. В зарубежных странах образовательные организации, в основном, регулируют содержание самостоятельно, опираясь на социальный заказ и рынок трудоустройства выпускников, требования к профессиональной сертификации специалистов. Некоторые зарубежные образовательные программы проходят добровольную общественную аккредитацию и сотрудничают при формировании своих программ с общественными организациями.

По сложившемуся ступеням подготовки – только в России допускается моноуровневый маршрут, вследствие сохранения традиционного для нашей страны уровня специалитета, при параллельной возможности обучаться по программам многоуровневого маршрута – бакалавриата и магистратуры. Число учебных заведений в России, реализующих ту или иную модель образовательного маршрута, примерно равно, что говорит о пригодности для российских условий

данных моделей обучения. В зарубежных странах подготовка будущих специалистов по информационной безопасности осуществляется только в рамках многоуровневой модели [8, с.116]. Вместе с тем, многоуровневость образования в области информационной безопасности является общей чертой всех рассматриваемых систем подготовки.

По критериям сопоставления функциональной подсистемы были выделены ключевые различия по отдельным образовательным технологиям, которые заключаются в формах организации учебного процесса, способах промежуточной и итоговой аттестации. Так, в Великобритании, Германии, Франции действует европейская переводная и накопительная система кредитов ECTS, когда каждый модуль, дисциплина, выпускная работа и другие зачетные единицы оцениваются в определенное количество баллов, из которых складывается по результатам обучения общая сумма. В США действует аналогичная накопительная система кредитов. Российское образование не использует подобные системы, или использует частично, в отдельных образовательных организациях. Промежуточная аттестация проходит в форме зачета или экзамена, итоговая – в виде защиты выпускной квалификационной работы и, по выбору вуза, государственного экзамена [8, с.117].

Следующее различие выделяется по соотношению объемов обязательных дисциплин и дисциплин по выбору обучающегося и заключается в том, что образовательные программы по информационной безопасности в Германии в большей степени дают свободу выбора студентам из предложенных дисциплин для изучения, во Франции, чаще всего, студентам предлагается выбрать две-три дисциплины из вариативного блока. В образовательных программах США и Великобритании количество дисциплин по выбору может значительно колебаться, в зависимости от конкретной образовательной организации, но, как правило, это не менее пяти дисциплин [8, с.117].

Дисциплины по выбору студента в российских программах предлагаются из нескольких групп (чаще всего от двух до пяти), из которых обучающийся

выбирает одну для изучения. Таким образом, предполагается, что студент самостоятельно формирует профиль обучения из предложенных вузом дисциплин. С другой стороны, чаще всего, студент уже при поступлении определяется с профилем и не может изменить его в процессе освоения образовательной программы.

В отдельных рассмотренных зарубежных образовательных программах формирование профиля, чаще всего, происходит несколько иначе. Предлагается список дисциплин (обычно более 6), за успешное изучение которых студент получает определенное количество баллов (кредитов). Студент должен выбрать из данного списка несколько дисциплин, чтобы в сумме набрать пороговый балл для выпускной аттестации.

Таким образом, в России и Франции выбор специализации регламентируемый, то есть образовательные организации, в силу небольшой вариативной части, сами предлагают образовательные программы соответствующего профиля, а студент выбирает специализацию (профиль) сразу при поступлении в университет. В Германии, Великобритании и США будущий специалист может выбрать в вариативной части во время обучения любую комбинацию изучаемых предметов, и тем самым самостоятельно формировать профиль подготовки.

Также различие можно выделить в формах реализации образовательного процесса. При наметившейся тенденции перехода к новым методикам, для отечественных образовательных организаций, тем не менее, характерны лекции, практические и лабораторные работы, семинары. В зарубежных образовательных программах, помимо традиционных лекций и семинаров, практическое обучение часто строится на выполнение проектов в небольших группах (обычно по 2-5 студентов), распространено привлечение специалистов из внешнего профессионального сообщества с целью разбора конкретных задач и решения актуальных проблем.

Вместе с тем, производственные практики, стажировки, а также реализуемые в процессе обучения проекты в рамках зарубежных образовательных программ по информационной безопасности ориентированы на рынок трудоустройства выпускников, чаще всего в бизнес-структурах (в большинстве случаев именно бизнес задает цель и содержание практики).

Различия, выявленные по критериям функциональной и организационно-управленческой подсистем, в целом, не являются специфичными для области образования будущих специалистов по информационной безопасности и, в большей степени, отражают особенности национальных систем профессионального образования (в ступенях подготовки, в управлении формированием образовательных программ, в образовательных технологиях, в ориентированности студенческих практик и стажировок на бизнес-структуры).

Ключевые различия, в первую очередь, выделяются по критериям содержательной подсистемы (направления подготовки и профили, содержание образования).

В странах, для которых характерна распространенность образовательных программ по информационной безопасности (США, Россия, Великобритания), реализуется подготовка по всем выделенным укрупненным блокам: по компьютерной безопасности, по законодательству в сфере информационных систем и защиты информации, по управлению информационной безопасностью, по безопасности информационных технологий и общим вопросам информационной безопасности, по безопасности компьютерных сетей, по расследованию компьютерных инцидентов, по криптографии. При этом в Германии мы не обнаружили отдельных программ по безопасности компьютерных сетей, расследованию компьютерных инцидентов и по криптографии. Образовательных программ, входящих в блок по законодательству в сфере информационной безопасности, не было выявлено во Франции. Вместе с тем, система профессионального образования специалистов по информационной безопасности во Франции значительное внимание уделяет аспектам

криптографической защиты информации и математическому циклу образования. Отличительной национальной особенностью Великобритании является существование подготовки магистров в области права, связанной с законодательными аспектам информационной безопасности [6, с.106].

Следующим ключевым различием содержательной компоненты является присутствие комбинированных образовательных программ, фактически включающих в себя несколько профилей: «Управление рисками и информационная безопасность», «Информационная безопасность и биометрика», «Компьютерная экспертиза и компьютерная безопасность», «Информационная безопасность и компьютерные сети» и других «смешанных» образовательных программ в США и Великобритании. Наличие подобных программ может свидетельствовать о востребованности в данных странах многопрофильных специалистов по информационной безопасности [6, с.106].

Набор образовательных программ, входящих в укрупненные блоки направлений подготовки и специальностей, различен для всех рассматриваемых стран. Например, в отечественной системе к образовательным программам, относящимся к блоку по законодательству в сфере информационных систем и защиты информации относятся программы, реализуемые по направлению подготовки «Безопасность информационных технологий в правоохранительной сфере», в Великобритании к программам данного блока относятся, среди прочего, программы «Законодательство в области безопасности информационных технологий» и «Создание компьютерных программ и законодательство», в системе подготовки специалистов Германии – «Информационное право и права интеллектуальной собственности». Таким образом, в каждой стране реализуются разные программы одного и того же блока.

Другой пример, блок по расследованию цифровых преступлений. В России реализуются образовательные программы по специализации «Компьютерная экспертиза при расследовании преступлений» направления подготовки «Безопасность информационных технологий в правоохранительной сфере», в

Великобритании и США популярны программы «Расследование компьютерных инцидентов», во Франции обнаружена программа данного блока – «Аудит безопасности и компьютерная экспертиза».

Итоговая иллюстрация по общим чертам и ключевым различиям систем профессионального образования в России, США, Великобритании, Германии, Франции представлена на рисунке 18.



<b>РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНО-СОПОСТАВИТЕЛЬНОГО АНАЛИЗА</b>						
<b>ОБЩИЕ ЧЕРТЫ</b>	<b>Цель подготовки</b>	Формирование у будущих выпускников компетенций, необходимых для квалифицированного решения задач обеспечения информационной безопасности в условиях существования угроз				
	<b>Образовательные организации</b>	Профессиональное образование будущих специалистов по информационной безопасности в России, США, Великобритании, Германии и Франции реализуется в образовательных организациях среднего, высшего и дополнительного образования.				
	<b>ППС</b>	Научно-педагогические кадры, имеющие ученую степень, базовое высшее образование, а также ведущие специалисты со стороны профессионального сообщества				
<b>КЛЮЧЕВЫЕ РАЗЛИЧИЯ</b>	<b>Содержательная подсистема</b>		<b>Функциональная подсистема</b>	<b>Организационно-управленческая подсистема</b>		
	<b>Направления подготовки, профили</b>	– Набор образовательных программ, входящих в укрупненные блоки направлений подготовки и специальностей, различен для всех рассматриваемых стран; – в Великобритании и США распространены комбинированные образовательные программы, фактически включающие в себя несколько специализаций; – в Великобритании присутствуют образовательные программы по правовым аспектам информационной безопасности при получении соответствующей степени магистра права	<b>Образовательные технологии</b>	– В Великобритании, Германии, Франции и США действует накопительная система кредитов; – по соотношению объемов обязательных дисциплин и дисциплин по выбору обучающегося (различно для всех рассматриваемых стран); – производственные практики, стажировки, а также реализуемые в процессе обучения проекты в рамках зарубежных образовательных программ ориентированы на рынок трудоустройства выпускников, чаще всего в бизнес-структурах (в большинстве случаев именно бизнес задает цель и содержание практики)	<b>Управление содержанием образовательных программ</b>	В России – частично формируются под влиянием ФГОС ВО, в зарубежных странах – устанавливаются образовательной организацией
	<b>Содержание образования</b>	– за рубежом в программах обучения отсутствуют дисциплин по инженерно-технической защите информации, распространенные в отечественных образовательных программах; – за рубежом в программах обучения присутствуют в значительном объеме дисциплины по компьютерной экспертизе, нераспространенные в отечественных образовательных программах; – набор дисциплин, входящих в схожие образовательные программы специалистов по информационной безопасности различен для всех рассматриваемых стран; – в большинстве зарубежных образовательных программах отсутствуют гуманитарные дисциплины; – в большинстве зарубежных образовательных программах широко распространены дисциплины экономического блока; – большинство зарубежных образовательных программ интегрировано с вендорскими образовательными курсами и содержательно ориентируются на будущую вендорнезависимую сертификацию выпускников.		<b>Целевая аудитория</b>	В зарубежных странах для поступления в магистратуру – необходимо наличие степени бакалавра по близким направлениям подготовки. В России – необходимо наличие степени бакалавра или специалиста по любому направлению.	<b>Сложившиеся ступени подготовки</b>

Рисунок 18 – Общие черты и ключевые различия систем профессионального образования в России, США, Великобритании, Германии, Франции

Сравнительно-сопоставительный анализ содержания отечественных и зарубежных образовательных программ по информационной безопасности, входящих в один и тот же укрупненный блок, позволяет сделать следующие основные выводы:

1. Совокупность дисциплин, входящих в образовательные программы блока, отличаются во всех рассматриваемых странах, что, вероятно, обусловлено социальным заказом профессионального сообщества, а также наличием или отсутствием управления содержанием образовательных программ.

2. В абсолютном большинстве зарубежных образовательных программах нами не было обнаружено дисциплин по изучению инженерно-технических методов обеспечения информационной безопасности, обязательных для образовательных программ по информационной безопасности в отечественных вузах.

3. В большинстве зарубежных образовательных программах нами не было обнаружено гуманитарных дисциплин, обязательных по отечественным образовательным стандартам или включенных дополнительно образовательными организациями России.

4. В большинстве зарубежных образовательных программах присутствуют в значительном объеме дисциплины по компьютерной экспертизе и расследованию цифровых преступлений, которые на данный момент не получили широкого распространения в отечественных образовательных программах.

5. В зарубежных образовательных программах широко распространены дисциплины экономического блока (менеджмент, управление бизнес-процессами и прочие);

6. В Великобритании присутствуют образовательные программы по направлениям подготовки, связанным с правовыми аспектам информационной безопасности при получении соответствующей степени (магистр права);

7. Во Франции широко распространены дисциплины (темы, модули) по криптографическим методам защиты информации и математическим циклом образования.

8. Значительная часть американских, британских, немецких и французских образовательных программ по информационной безопасности интегрирована с вендорскими образовательными курсами и содержательно ориентируются на будущую вендорнезависимую сертификацию выпускников.

### **2.3 Модернизация содержательной составляющей отечественной системы профессионального образования по информационной безопасности**

Сравнительно-сопоставительный анализ систем профессионального образования специалистов по информационной безопасности (§§1.2-2.1) позволил, с одной стороны, выявить критерии для сопоставления образовательных систем в России, США, Великобритании, Германии и Франции (§2.2), выделить общие черты и ключевые различия систем подготовки, а с другой стороны, используя рассмотренные методологические подходы, сформулировать отдельные компоненты модернизации отечественной системы подготовки специалистов по информационной безопасности. В данной главе мы не ставим задачу разработать конкретные методические рекомендации или педагогические условия по использованию тех или иных образовательных технологий, по методике преподавания отдельных тем информационной безопасности. Наша задача – обосновать возможность модернизации содержательной составляющей отечественной системы профессионального образования будущих специалистов по информационной безопасности с учетом позитивного зарубежного опыта.

Компоненты модернизации содержательной составляющей отечественной системы профессионального образования специалистов и механизмы их реализации, в рамках нашего исследования, позволили понять системный и информационный подходы, каждый из которых сделали возможным увидеть решение одной или нескольких подзадач.

В §2.1 с помощью *историко-логического анализа* развития информационных технологий (прежде всего компьютерных систем и сетей) показано, что отечественная ИТ-отрасль в последние 30 лет существенно отстает от западной индустрии. Об этом говорят современные стратегические документы, многие современные исследователи и эксперты информационной и экономической отраслей [45, 51, 67, 70, 95]. Сегодня Россия находится практически полностью в «цифровой зависимости» от западных разработок [43].

Однако уже ведется работа по внедрению отечественного программного обеспечения в органах исполнительной власти и государственных внебюджетных фондах Правительства РФ в соответствии с распоряжением от 26 июля 2016 года №1588-р. С 2017 года, учитывая важность вопросов импортозамещения и социальный характер задачи Министерство образования и науки РФ проводило аналогичную работу по планированию перехода на использование отечественного программного обеспечения во всех подведомственных образовательных организациях с целью преодоления зависимости от иностранного программного обеспечения» и формирования у обучающихся отложенного спроса на российские программные разработки (что указано в письме зам.директора департамента управления программами и конкурсных процедур Минобрнауки России №03-1463 от 10.08.2017 г.).

В то же время, в Доктрине информационной безопасности РФ отмечено, что наблюдается недостаточность эффективных научных исследований, низкий уровень отечественных разработок и недостаточное кадровое обеспечение в области информационной безопасности [70].

Одним из механизмов, способствующих построению «прорывных» технологий, которые, в свою очередь, смогут развить собственную исследовательскую инфраструктуру и существенно повысить конкурентоспособность отечественных разработок в области информационной безопасности, на наш взгляд, должен стать своевременный переход на интеграцию системы профессионального образования ИТ-специалистов в целом, специалистов по защите информации, в частности, с профессиональным сообществом (прежде всего частным сектором).

С точки зрения *системного подхода* – задачей ставилось выявить элементы системы, в том числе системообразующие, и отношения рассмотренных процессов подготовки будущих специалистов с позиции целостности. В §2.2 было определено, что систему профессионального образования специалистов по информационной безопасности можно рассматривать как совокупность

содержательной, функциональной и организационно-управленческой подсистем. Также были определены элементы каждой подсистемы, имеющие значение при проведении сравнительно-сопоставительного анализа. В свою очередь выделенные элементы, в рамках диссертационного исследования, рассматриваются как критерии сопоставления систем подготовки в области информационной безопасности в разных странах. Основная цель профессиональной подготовки будущих специалистов по информационной безопасности, являясь системообразующим элементом, также становится критерием сравнительно-сопоставительного анализа.

С точки зрения *информационного подхода* мы рассматриваем каждую образовательную программу по информационной безопасности в разных странах как информационную модель. Задачей информационного подхода было выделить и проанализировать информационные модели, необходимые для описания системы профессионального образования специалистов по информационной безопасности и проведения сравнительного анализа.

Таким образом, в рамках последней задачи диссертационного исследования, сформулированной как «выявить и обосновать компоненты модернизации содержательной составляющей отечественной системы профессионального образования по информационной безопасности с учетом позитивного зарубежного опыта и экспериментально проверить влияние изучения вендорского образовательного курса на уровень готовности студентов к будущей профессиональной деятельности» нами не планируется возможность «жесткого» переноса зарубежного опыта в отечественную систему, а предполагается поиск возможных компонентов модернизации отечественной системы профессионального образования и механизмов их реализации.

В таблице 2 представлено соответствие решаемых подзадач диссертационного исследования и результатов сравнительно-сопоставительного анализа выбранным методологическим подходам.

Таблица 2 – Результаты сравнительно-сопоставительного анализа в соответствии с методологическими подходами

Методологический подход к анализу подготовки будущих специалистов по информационной безопасности	Решаемая подзадача	Результаты сравнительно-сопоставительного анализа
Историко-логический подход	Установить причинно-следственные связи процессов формирования системы профессионального образования специалистов по информационной безопасности	<p>Выделены этапы формирования профессионального образования специалистов по информационной безопасности в РФ:</p> <ul style="list-style-type: none"> <li>– этап подготовки кадров, способных решать фрагментарные вопросы защиты информации в «закрытых» ведомственных учреждениях;</li> <li>– этап подготовки специалистов по информационной безопасности в учреждениях высшего образования по «закрытым» программам;</li> <li>– этап появления отдельных «открытых» образовательных программ по информационной безопасности в учреждениях высшего образования;</li> <li>– этап массовой реализации программ по информационной безопасности в образовательных учреждениях разного уровня;</li> <li>– этап подготовки специалистов по информационной безопасности по сферам деятельности.</li> </ul>
	Выявить социальный заказ общества на подготовку современных специалистов по информационной безопасности, применен анализ социально-экономических предпосылок	<p>В связи с существенным отставанием отечественной ИТ-отрасли необходимы «прорывные» технологии, в том числе в сфере защиты информации.</p> <p>В связи с массовой информатизацией общества процессы обеспечения информационной безопасности становятся все более востребованными в бизнес-сообществе, которое и формирует основной социальный заказ на специалистов по защите информации в развитых странах (в том числе и в России).</p> <p><i>Формулируется компонент модернизации содержательной составляющей:</i></p> <ul style="list-style-type: none"> <li>– Переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества</li> </ul>

## Продолжение Таблицы 2

Методологический подход к анализу подготовки будущих специалистов по информационной безопасности	Решаемая подзадача	Результаты сравнительно-сопоставительного анализа
Системный подход	Выявить элементы системы, в том числе системообразующие, рассмотренных процессов профессиональной подготовки будущих специалистов с позиции целостности	Выделены критерии сопоставления, соответствующие подсистемам образовательной системы: - <i>содержательная</i> (направления подготовки будущих специалистов по ЗИ; содержание учебных планов, модулей/дисциплин образовательных программ); - <i>функциональная</i> (образовательные организации, образовательные технологии, ППС, целевая аудитория); - <i>организационно-управленческая</i> (управление содержанием образовательных стандартов, сложившиеся ступени подготовки); Цель подготовки будущих специалистов – системообразующий элемент системы
Информационный подход	Выделить и проанализировать информационные модели, необходимые для описания системы профессионального образования специалистов по информационной безопасности и проведения сравнительного анализа	Проанализировано около 400 отечественных и зарубежных образовательных программ по информационной безопасности, включая учебные планы, программы дисциплин и практик и др. <i>Формулируются компоненты модернизации содержательной составляющей:</i> – фрагментарное изменение содержания образовательных программ – интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров



Рассмотрим компоненты модернизации содержательной составляющей отечественной системы профессионального образования специалистов и механизмы их реализации подробнее (рисунок 19).

Компоненты модернизации	Механизмы реализации компонента
<p>1) Переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества</p>	<ul style="list-style-type: none"> <li>– включение в образовательные программы дисциплин (тем, модулей), связанных с обеспечением ИБ в бизнес-структурах и электронной коммерции;</li> <li>– расширение сотрудничества образовательных организаций с бизнесом</li> </ul>
<p>2) Фрагментарное изменение содержания образовательных программ</p>	<ul style="list-style-type: none"> <li>– включение в образовательные программы дисциплин (тем, модулей), формирующих способности проведения компьютерной экспертизы и расследованию цифровых инцидентов;</li> <li>– включение в образовательные программы дисциплин (тем, модулей), связанных с правоприменительными технологиями в области информационной безопасности;</li> <li>– включение в образовательные программы дисциплин (тем, модулей), связанных с обеспечением ИБ в бизнес-структурах и электронной коммерции</li> </ul>
<p>3) Интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров</p>	<ul style="list-style-type: none"> <li>– сотрудничество с ИТ-компаниями, предлагающими собственные образовательные ресурсы;</li> <li>– внедрение вендорских образовательных курсов в соответствующие дисциплины образовательных программ по информационной безопасности с последующей сертификацией</li> </ul>

Рисунок 19 – Компоненты модернизации содержательной составляющей отечественной системы образования специалистов и механизмы их реализации.

*Переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества.*

Профессор Г.И. Маргаров отмечает, что до конца XX века в нашей стране понятия «защита информации» и «обеспечение информационной безопасности» приравнивались к соблюдению режима секретности сведений, составляющих государственную тайну и практически не распространялась на безопасность информации, конфигурирующей в частных организациях [58]. Данный аспект нашел свое отражение в сегодняшней системе обучения специалистов по информационной безопасности: в большинстве отечественных образовательных программах уделяется значительное внимание на организационно-правовые и инженерно-технические методы обеспечения информационной безопасности. Фактически, такой подход направлен на обеспечение конфиденциальности информации (в том числе государственной тайны).

Однако за последние десятилетия широкая информатизация всех видов деятельности в нашей стране трансформирует требования к уровню профессиональной подготовки будущих специалистов. В настоящее время необходимы специалисты, владеющие необходимыми компетенциями обеспечения информационной безопасности не столько в регламентированных рамках, сколько в широком поле деятельности, в том числе при взаимодействии с бизнес-сообществом, в развитии электронной коммерции и защите интеллектуальной собственности. Такие методы и средства должны быть направлены на обеспечение всех составляющих информационной безопасности (конфиденциальности, доступности и целостности) на равноправной основе.

Проведенный анализ зарубежных национальных систем профессионального образования будущих специалистов по информационной безопасности показывает, что во всех странах практически все образовательные программы в обязательном цикле обучения включают ряд дисциплин, связанных с бизнес-процессами, обеспечением информационной безопасности в информационных

системах бизнес-структур [114, с.21].

Мы полагаем, что изменение содержательной компоненты при помощи механизма внедрения в образовательные программы дисциплин, связанных с обеспечением безопасности в информационных системах бизнес-структур и безопасности электронной коммерции, сможет компенсировать недостаточные знания будущих специалистов в данной области [4, с.230; 110, с.51].

Вместе с тем, важно расширение сотрудничества образовательных организаций с бизнесом. В широком смысле на это обращают внимание ученые-компаративисты: страны с ведущими экономиками мира не только в профессиональном образовании, но уже и в процессе школьного обучения, ориентируются на сотрудничество образовательных организаций с бизнес-структурами. Так, В.И. Петрищев и Т.П. Грасс отмечают, что данное взаимодействие «...в разных странах осуществляется с учетом местных условий и в разных формах: от участия в модернизации учебных планов до создания мини-предприятий и развития механизма государственно-частного партнерства» [30, с.245]. Безусловно, это актуально и на уровне высшего образования, в частности в профессиональной подготовке специалистов по обеспечению безопасности данных, когда интеграция обучения с профессиональной средой способствует формированию необходимых бизнес-навыков у будущих выпускников (среди которых обоснование необходимости проведения мероприятий по защите информации перед руководством компании, обоснование экономической эффективности выбранных средств защиты, навыки работы с инструментами управления рискам и обеспечения информационной безопасности ERP-систем и прочее), увеличивает их вовлеченность в профессиональное сообщество.

#### ***Фрагментарное изменение содержания образовательных программ.***

Одним из основных различий образовательных программ специалистов по информационной безопасности в России и рассматриваемых зарубежных странах по содержательной подсистеме является наличие и большая распространенность в зарубежных странах программ и дисциплин по компьютерной экспертизе и расследованию компьютерных инцидентов [4, с.230, 12, с.335-336].

Такое различие обусловлено в историческом аспекте формированием деятельности по обеспечению информационной безопасности (§2.1). Подготовка будущих специалистов по компьютерной экспертизе в рассматриваемых зарубежных странах раньше перестала иметь «закрытый» характер, сегодня многие вузы предоставляют свои образовательные ресурсы в данном направлении [12, с.336]. Как показано в 1-й главе, такие образовательные программы в Великобритании и США можно выделить в самостоятельный укрупненный блок, они востребованы среди студентов как бакалавриата, так и магистратуры. Образовательные программы в области информационной безопасности во Франции и Германии также включают в себя дисциплины, связанные с проведением экспертизы компьютерных систем и расследованием преступлений в компьютерной сфере.

К следующему ключевому различию в содержательной компоненте образовательных программ, вытекающему из выше озвученного, можно отнести незначительный объем дисциплин (тем, модулей), посвященных проблемам правоприменительных инструментов в области обеспечения безопасности данных, а также защиты информационной сферы личности и общества в отечественных образовательных программах [4, с.230; 12, с.336].

Необходимо отметить, что федеральные органы государственной власти прилагают большие усилия по укреплению законодательства в области информационной безопасности РФ, которое является частью национальной безопасности.

Вместе с тем, практически все отечественные образовательные программы содержат дисциплины по правовой защите информации, в рамках которых рассматривается базовое законодательство в сфере информационной безопасности, однако, продолжает остро стоять проблема правоприменительных технологий в информационной сфере, в частности в области информационной безопасности [4, с.230].

Специалист по защите информации в любой организации (государственной или частной) в процессе выполнения своих должностных обязанностей должен

строго соответствовать регламентирующим нормам права. И если в случае защиты коммерческой тайны у специалиста достаточно свободы выбора относительно самих сведений, составляющих тайну и методов их защиты, то в случае с персональными данными существует необходимость строго соблюдать требования регуляторов: ФСТЭК, ФСБ, Роспотребнадзора. Чаще всего эти требования не очевидны и вызывают множество сложностей и спорных вопросов, в том числе по части реализации закона «О персональных данных» [59] и других норм [55]. До сегодняшнего момента еще не закончено формирование основ законодательства в сфере информационной безопасности: принимаются новые законы, например, регулирующие вопросы защиты информации в критической инфраструктуре; ранее принятые претерпевают существенные корректировки: в части защиты персональных данных, лицензировании деятельности в сфере информационной безопасности, требований Роскомнадзора по ограничению интернет-ресурсов, содержащих информацию, распространение которой в РФ запрещено и других [12, с.336].

Мы полагаем, что в рамках реализации общепрофессиональных или профессиональных компетенции бакалавров и магистров по информационной безопасности и специалистов по защите информации, связанных с анализом нормативно-правовых актов, навыками работы в рамках регламентной документации, важно уделять достаточное внимание обоснованию и принятию действий по реализации правовых норм, а также составлению нормативно-правовых документов (в том числе политик и концепций информационной безопасности).

В подходе к решению данной проблемы интересен опыт по подготовке специалистов по информационной безопасности в Великобритании, где можно выделить отдельный укрупненный блок образовательные программы, связанные с законодательством в области информационной безопасности. Студенты имеют возможность получить степень магистра права в сфере информационной безопасности. Кроме того, образовательные программы других укрупненных блоков содержат ряд дисциплин, связанных с правовыми аспектами защиты

информации и правоприменительными технологиями [4, с.230; 12, с.336].

Таким образом, целесообразно в рамках отдельных дисциплин по правовой защите информации акцентировать внимание также и на правоприменительные технологии в области информационной безопасности [12, с.336].

Отметим, что модернизации содержательной компоненты образовательных программ также требует рассмотренная выше переориентация на потребности коммерческих структур и бизнес-сообщества выступающая как компонент модернизации содержательной составляющей отечественной системы профессионального образования специалистов по информационной безопасности [4, с.230].

Компенсировать недостаточность необходимых в современном обществе вышеуказанных компетенций специалиста по защите информации (защита информации в бизнес-структурах, расследованию компьютерных преступлений, правоприменительных технологий) возможно введением отдельных дисциплин в образовательные программы, связанные с информационной безопасностью.

Таким образом, механизмом реализации первого и второго компонента модернизации содержательной составляющей образовательных программ по обеспечению безопасности данных является включение дисциплин (тем, модулей) по обеспечению информационной безопасности в бизнес-структурах, компьютерной экспертизе и расследованию компьютерных инцидентов. Примером реализации механизмов являются разработанные учебные планы основных образовательных программ 10.03.01 «Информационная безопасность», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» [37], которые включают в себя дисциплины «Расследование компьютерных инцидентов», «Компьютерная экспертиза», «Избранные вопросы по информационной безопасности». В приложении К представлена аннотация к рабочей программе дисциплины «Избранные вопросы по информационной безопасности», в которую включены темы по расследованию цифровых преступлений, менеджменту информационной безопасности в бизнесе, информационным угрозам бизнеса, обеспечение кибербезопасности данных и

безопасности ИТ-систем в бизнесе.

Однако в условиях постоянной модернизации отечественной системы профессиональной подготовки специалистов по информационной безопасности, в рамках которой принимаются новые образовательные стандарты, изменяются перечень видов деятельности и компетенций, корректируются внутренние регламенты образовательных организаций относительно формирования образовательных программ, в том числе учебных планов, нам не представилось возможным провести экспериментальную проверку эффективности внедрения указанных рабочих программ дисциплин. Так, частые корректировки учебных планов не позволяют выполнять необходимые равные исходные условия для контрольной и экспериментальной группы при формировании групп из разных наборов учебных лет. Вместе с тем, формирование общепрофессиональных компетенций в отдельных дисциплинах не позволяет их реализацию в блоке дисциплин по выбору для формирования контрольной и экспериментальной группы одного года набора.

***Интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров.***

Анализ зарубежного опыта показал (§1.4), что образовательные программы по информационной безопасности при изучении соответствующих дисциплин (тем, модулей) зачастую опираются на курсы популярных ИТ-компаний, с продукцией которых будущим специалистам с высокой долей вероятности придется работать в процессе своей профессиональной деятельности. К таким компаниям, среди прочих, относится компания Cisco. Несмотря на то, что компания американская, как уже отмечалось выше, ее образовательные курсы внедряются в образовательные программы ИТ-направлений и французских, и немецких, и британских вузов. Это общемировая практика, так как значительная часть телекоммуникационных сетей не только в США, но и в Европе и России построены с использованием оборудования Cisco [88]. Надежность этих программных и аппаратных средств с точки зрения безопасности использования

при обработке информации, в том числе и в государственных органах России, подтверждена ФСТЭК РФ. По состоянию на май 2018 года «Государственный реестр сертифицированных средств защиты информации» [108] содержит список из более чем 180 сертификатов на решения компании Cisco.

В ТГУ имени Г.Р. Державина с 2017-2018 учебного года в рамках дисциплины «Основы информационной безопасности» направления 10.03.01 «Информационная безопасность» у студентов 1-го курса введен учебный курс начального уровня «Введение в кибербезопасность» (аннотация к рабочей программе по дисциплине с внедрением – приложение Л). Студенты, успешно прошедшие итоговое тестирование, получают международный сертификат (пример студенческого сертификата – приложение М).

С 2018-2019 учебного года студенты изучают дисциплину «Системы защиты информации в мире» с внедрением учебного курса среднего уровня «Основы кибербезопасности» (аннотация к рабочей программе по дисциплине – приложение Н, пример студенческого сертификата – приложение П).



## **2.4 Опытнo-экспериментальная работа по интеграции образовательных программ с вендорским учебным курсом**

Среди перечисленных возможных компонентов модернизации содержательной составляющей отечественной системы подготовки специалистов по информационной безопасности (переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества; фрагментарное изменение содержания образовательных программ; интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров) для проведения опытнo-экспериментальной работы был выбран третий компонент в виду объективных сложностей опытнo-экспериментальной проверки механизмов совершенствования по первому и второму компоненту. Для проверки результатов обучения по одному из внедренных механизмов была проведена опытнo-экспериментальная работа по оценке влияния изучения сертифицированного вендорского образовательного курса на уровень готовности студентов старших курсов к будущей профессиональной деятельности.

Опытнo-экспериментальная работа по интеграции образовательных программ с вендорским учебным курсом проводилась на базе ФГБОУ ВО «Тамбовский государственный университет имени Г.Р. Державина». В исследовании приняли участие 81 обучающийся, среди которых студенты 4-го курса направления подготовки 10.03.01 «Информационная безопасность» и студенты 4-го курса специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», в течение 2018-2019, 2019-2020 и 2020-2021 учебных лет. Исследование по интеграции образовательных программ с вендорским учебным курсом было проведено на примере курса «Основы кибербезопасности» (Cybersecurity Essentials) Сетевой академии Cisco [2, с.95].

Студенты обучались по программе с внедрением учебного курса среднего уровня «Основы кибербезопасности» в дисциплину «Системы защиты информации в мире». Данная дисциплина изучается студентами образовательных программ 10.03.01 «Информационная безопасность» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в течение трех семестров (5-7 семестры). Пятый семестр изучается тематический блок «История становления системы обеспечения безопасности в информационной сфере в России», в шестой – «Современная система защиты информации за рубежом» и в седьмой – «Зарубежный взгляд на обеспечение кибербезопасности». В рамках третьего блока предполагается изучение вендорского учебного курса.

Группы обучающихся были поделены на две подгруппы: первая изучала третий блок дисциплины с внедрением вендорского курса Сетевой академии Cisco «Основы кибербезопасности», вторая – продолжила обучение по тем же темам, что и в вендорском курсе, но традиционными методами обучения (лекции, практические и лабораторные работы с преподавателем) [2, с.95]. Таким образом, в экспериментальную группу (ЭГ) вошли 49 студентов, в контрольную (КГ) – 32.

Целью проведения опытно-экспериментальной работы стало изучение уровня готовности студентов к будущей профессиональной деятельности [2, с.95]. Л.С. Моцарь понятие готовность студента к профессиональной деятельности рассматривает «как результат накопления качественных личностных изменений и обретения профессиональной компетентности субъектом будущей профессиональной деятельности» [64, с.111].

В работе Т.А. Лавиной и Л.А. Ильиной уточняется, что «готовность к осуществлению профессиональной деятельности стали оценивать, используя понятия «компетенция» и «компетентность», а их формирование посредством знаний, умений, навыков, свойств личности и т.д.» [49, с.114].

Подробный анализ подходов к трактовке понятия «готовность к профессиональной деятельности» представлен в диссертации М.В. Храмовой, где автор приходит к выводу, что «все исследователи рассматривают готовность как необходимую предпосылку успешной деятельности специалиста, которая

предполагает наличие профессионально значимых качеств и свойств личности» [109, с.47-48].

Мы рассматриваем готовность студентов к будущей профессиональной деятельности как комплекс, включающий мотивационный, когнитивный, деятельностный, эмоционально-оценочный компоненты.

Таким образом, уровни готовности (низкий, средний и высокий) характеризуются по выделенным компонентам (критериям): мотивационный (проявление интереса к учебно-познавательной и профессиональной деятельности и осознание значимости изучения вендорских курсов), когнитивный (уровень теоретической подготовки), деятельностный (способность к решению задач информационной безопасности в условиях существования угроз), эмоционально-оценочный (сформированность профессиональной и личностной компетентности) [2, с.95].

Методики, по которым были проведены диагностические исследования, представлены в таблице 3.

Таблица 3 – Критерии и диагностический инструментарий уровня готовности студентов к будущей профессиональной деятельности.

Критерии	Показатели	Методики диагностики
Мотивационный	Осознание значимости изучения вендорского курса для повышения личностной конкурентоспособности студента	Экспресс-диагностика личностной конкурентоспособности (Фетискин Н.П.)
	Проявление интереса к профессиональной деятельности	Методика для диагностики учебной мотивации студентов (А.А.Реан и В.А.Якунин, модификация Н.Ц.Бадмаевой)
	Проявление интереса к учебно-познавательной деятельности	
Когнитивный	Уровень теоретической подготовки	Вводное тестирование Итоговое тестирование
Деятельностный	Способность к решению задач информационной безопасности в условиях существования угроз	Самооценка студентов профессиональных умений и навыков
Эмоционально-оценочный	Представление о процессе обучения	Профессиональный личностный опросник (Филиппова К.А.)
	Видение перспектив профессионального и карьерного роста	
	Уверенность в себе и в своей будущей профессиональной эффективности	

Характеристики компонентов готовности студентов к будущей профессиональной деятельности на низком, среднем и высоком уровнях ее сформированности в таблице 4.

Таблица 4 – Характеристика компонентов готовности студентов к будущей профессиональной деятельности на низком, среднем и высоком уровнях ее сформированности

1	2	3	4
Показатель сформированности	Уровни выраженности		
	Низкий	Средний	Высокий
<b>Мотивационный компонент</b>			
Осознание значимости изучения вендорского курса для повышения личностной конкурентоспособности студента	Незначительный интерес к изучению вендорских курсов, не развита личностная конкурентоспособность	Фрагментарный интерес к изучению вендорских курсов, частично развита личностная конкурентоспособность	Устойчивый интерес к изучению вендорских курсов, развита личностная конкурентоспособность
Проявление интереса к профессиональной деятельности	Слабо выраженная профессиональная мотивация	Ситуативная профессиональная и мотивация	Ярко выраженная профессиональная и мотивация
Проявление интереса к учебно-познавательной деятельности	Слабо выраженная учебно-познавательная мотивация	Ситуативная учебно-познавательная мотивация	Ярко выраженная учебно-познавательная мотивация
<b>Когнитивный компонент</b>			
Уровень теоретической подготовки	Фрагментарные знания принципов обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз	Достаточный объем знаний о принципах обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз	Систематизированные, глубокие и полные знания принципов обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз
<b>Деятельностный компонент</b>			
Способность к решению задач информационной безопасности в условиях существования угроз	Фрагментарные умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности	Достаточный уровень сформированности навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности	Высокий уровень сформированности навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности

## Продолжение Таблицы 4

1	2	3	4
Показатель сформированности	Уровни выраженности		
	Низкий	Средний	Высокий
Эмоционально-оценочный компонент			
Представление о процессе обучения	Негативная направленность представлений о целях обучения в вузе, в целом недостаточная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента	Нейтральная направленность представления о целях обучения в вузе, в целом достаточная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента	Позитивная направленность представления о целях обучения в вузе, адекватная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента
Видение перспектив профессионального и карьерного роста	Смутное представление о перспективах и планах относительно личной профессиональной карьеры	Частичное видение перспектив и планов относительно личной профессиональной карьеры	Четкое видение перспектив и выраженная способность планировать личную профессиональную карьеру
Уверенность в себе и в своей будущей профессиональной эффективности	Профессиональное будущее представляется неопределенным, существует ее неоднозначность, даже в виде представления.	Представление о своей будущей профессиональной эффективности в целом оптимистичны, но имеются сомнения	Устойчивое оптимистическое представление о своей будущей профессиональной эффективности

*Констатирующий этап опытно-экспериментальной работы.*

На констатирующем этапе опытно-экспериментальной работы в каждом учебном году диагностировался исходный уровень готовности студентов к будущей профессиональной деятельности. Опишем полученные данные по использованным в ходе эксперимента методикам в ЭГ и КГ.

Перейдем к анализу исходного уровня развития **мотивационного критерия.**

Методика *«Экспресс-диагностика личностной конкурентоспособности»* (Н.П. Фетискин)[105, с. 272-273].

В рамках нашего исследования данный показатель рассматриваем в ключе осознания значимости изучения вендорской образовательной программы для повышения личностной конкурентоспособности студентов старших курсов, в том числе при будущем трудоустройстве.

Обучающимся предлагалось оценить степень проявления 11 психологических качеств по шкале от -3 до +3 (в левой части качество, которым свойственны баллы с отрицательным, а в правой – с положительным знаком). При обработке результатов выяснилось, что градация, предлагаемая в интерпретации, не совсем корректна. Поэтому нами была разработана собственная шкала, максимально приближенная к предлагаемой автором.

Данное исследование показало, что 21,9 % студентов КГ и 31,35 % студентов ЭГ имеют средний уровень личностной конкурентоспособности, незначительным уровнем обладают по 56,3 % в обеих группах. У 21,9 % студентов КГ и 12,5 % ЭГ – незначительное преобладание свойств, препятствующих проявлению личностной конкурентоспособности [2, с.95-96].

В рамках оценки готовности студентов к будущей профессиональной деятельности будем считать, что у студента не развита личностная конкурентоспособность и он проявляет незначительный интерес к изучению вендорских курсов и в случае, если у него будут преобладать свойства, препятствующие проявлению личностной конкурентоспособности в любой степени; частично развита, если у испытуемого обнаружили незначительный уровень; и, что личностная конкурентоспособность развита, а студент проявляет устойчивый интерес к изучению вендорских курсов, в случае, если у студента обнаружили средний или высокий уровень личностной конкурентоспособности.

Соответственно, личностная конкурентоспособность развита у 21,9 % студентов КГ и 31,35 % студентов ЭГ. Проявили частично развитую конкурентоспособность 56,3 % студентов в КГ и ЭГ. Низкий уровень по данному показателю обнаружился у 21,9 % студентов КГ и 12,5 % ЭГ [2, с.95-96].

Проведенная диагностика показывает, что показатель – осознание значимости изучения вендорских курсов для повышения личностной конкурентоспособности студента – мотивационного критерия в КГ и ЭГ имеет *средний уровень* развития.

*Методика для диагностики учебной мотивации студентов (А.А. Реан и В.А. Якунин, модификация Н.Ц. Бадмаевой) [20, с.151-154].*

Студентам предлагалось оценить 34 мотива учебной деятельности по 5-балльной системе. Результат обрабатывался подсчетом среднего значения по каждой шкале опросника.

Целью проведения диагностики по данной методике в рамках нашего исследования является изучение уровня профессиональной и учебно-познавательной мотивации студентов [2, с.96]. Будем считать, что у обучающихся слабо выраженная профессиональная или учебно-познавательная мотивация (низкий уровень), если средний балл по соответствующем шкале будет менее 2,3333; ситуативная профессиональная или учебно-познавательная (средний уровень) мотивация средний балл в диапазоне от 2,3333 до 3,6666; ярко выраженная профессиональная или учебно-познавательная мотивация (высокий уровень) – более 3,6666.

На рисунке 20 представлено процентное соотношение по семи шкалам мотивов в КГ и ЭГ, в выборку вошли обучающиеся, у которых соответствующий мотив имеет средний балл выше 4,0.



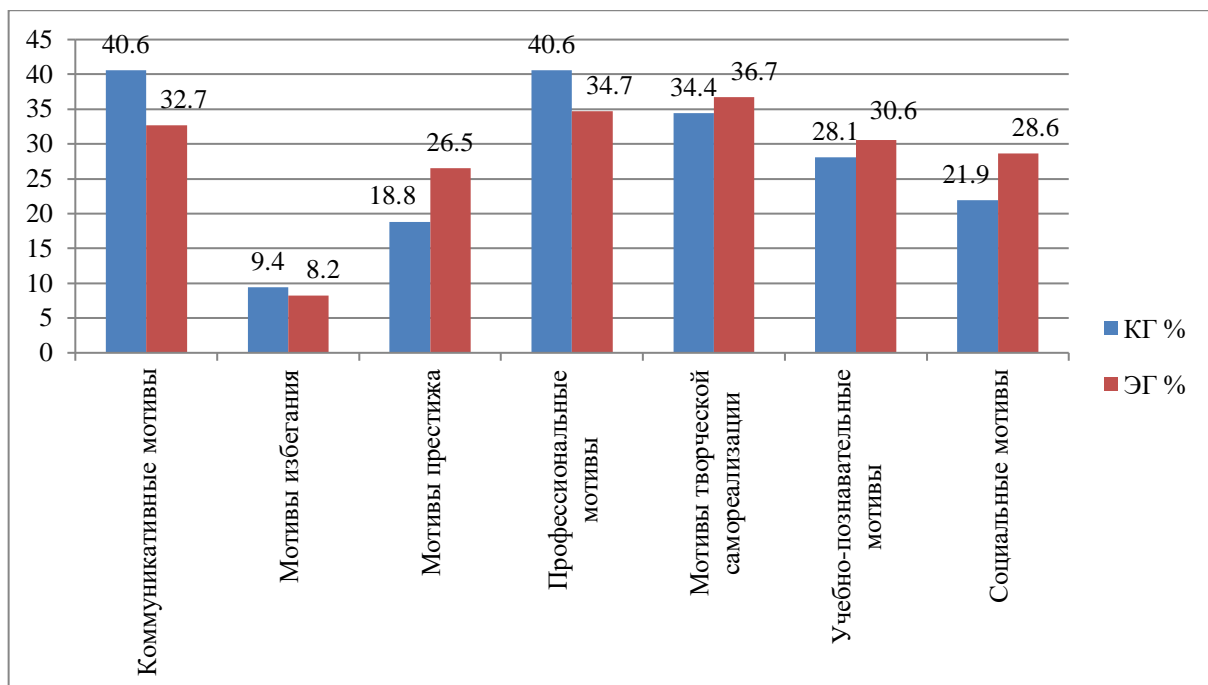


Рисунок 20 – Распределение мотивов по шкалам в КГ и ЭГ на констатирующем этапе эксперимента, %

Определение уровня профессиональной мотивации показывает, что у 18,8 % КГ и 24,5 % ЭГ мотивация выражена слабо, ситуативная мотивация присуща 25,0 % КГ и 34,7 % ЭГ. Ярко выраженной профессиональной мотивацией обладают 56,2 % студентов КГ и 40,8 % ЭГ [2, с.96]. Таким образом, усредненное значение по группе данного показателя мотивационного критерия в ЭГ и КГ находится на *среднем уровне*.

Схожая ситуация складывается по итогам диагностики учебно-познавательных мотивов. Низкий уровень имеют 25 % студентов ЭГ и 21,9 % КГ, мотивация на среднем уровне – у 37,5 % ЭГ и 40,6 % КГ и на высоком – у 37,5 % в обеих группах [2, с.96]. Следовательно, показатель «проявление интереса к учебно-познавательной деятельности» мотивационного критерия в ЭГ и КГ, в целом по группам, до проведения изучения вендорского учебного курса имеет *средний уровень*.

Это может говорить о том, что студенты исходно, в целом, заинтересованы в выбранной специальности и считают изучаемые дисциплины значимыми для своей будущей профессиональной деятельности, однако около половины

обучающихся, не имеющих выраженной учебно-познавательной и профессиональной мотивации, сомневаются, что получаемые знания пригодятся в будущей профессии или вообще не уверены, что хотят стать специалистами по защите информации.

С целью выявления исходного уровня **когнитивного критерия** студентам КГ и ЭГ предлагалось пройти вводное тестирование (приложение Р) для определения уровня теоретических знаний.

Данные результатов тестирования показали, что знания принципов обеспечения защиты информации, источников угроз, современных методов и средств защиты от угроз информационной безопасности на низком уровне обнаружались у 18,8 % обучающихся КГ и 12,2 % ЭГ, средний уровень продемонстрировали значительная часть студентов КГ и КГ – 68,8 % и 75,5 % соответственно. Высоким уровнем знаний основ информационной безопасности обладают чуть более 12 % студентов обеих групп [2, с.97].

Результаты проведенной диагностики уровня когнитивного критерия на констатирующем этапе показали, что и в КГ и в ЭГ данный показатель находится на *среднем уровне*.

Для определения уровня развития показателя **деятельностного критерия** обучающимся была предложена анкета самооценки умений и навыков применения современных подходов к технологиям и методам обеспечения информационной безопасности (приложение С), среди которых: навыки использования многофакторной аутентификации для защиты личной учетной записи, навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи, умение применять методы стеганографии, умение выяснить пароль пользовательских учетных записей с помощью специальных утилит, навык проверки электронного документа и цифровой подписи и других. Собственные умения и навыки обучающимся необходимо было оценить по 10-бальной шкале.

В таблице 5 представлен средний балл по каждому умению и навыку в КГ и ЭГ.

Таблица 5 – Результат самооценки студентов умений и навыков на констатирующем этапе эксперимента.

	<b>Умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности</b>	<b>КГ</b>	<b>ЭГ</b>
1.	Навыки поиска вакансий в сфере информационной безопасности.	5,3	5,2
2.	Умение оценить угрозы, исходящие от кибератак	5,9	5,9
3.	Навыки использования многофакторной аутентификации для защиты личной учетной записи	7,0	6,8
4.	Навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи	7,3	7,3
5.	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	7,0	6,2
6.	Навыки применения мер обеспечения безопасности на хостовой машине методом назначения разрешений с использования символического и абсолютного обозначения	5,7	5,6
7.	Умение выявлять угрозы и уязвимости в системе с помощью средства для анализа топологии сетевой инфраструктуры (сканера портов)	5,5	5,8
8.	Умение применять методы стеганографии (сокрытия документа внутри графического файла)	5,1	5,1
9.	Умение выяснить пароль пользовательских учетных записей с помощью специальных утилит	5,6	5,8
10.	Навыки использования цифровых подписей для подписания юридического документа	5,9	5,8
11.	Навыки проверки электронного документа и цифровой подписи	5,9	6,1
12.	Умение создать собственную цифровую подпись	6,8	6,5
13.	Умение использовать протокол SSH для удаленного подключения к хосту	5,9	5,6
14.	Умение использовать протокол Telnet для удаленного подключения к хосту	6,2	5,6
15.	Умение использовать инструменты повышения надежности операционной системы	7,1	7,1
16.	Навыки анализа примененных инструментов повышения надежности операционной системы и интерпретации предупреждений и рекомендаций системы	6,3	6,8

Будем считать, что студент обладает фрагментарными умениями и навыками применения современных подходов к технологиям и методам обеспечения информационной безопасности (низкий уровень) в случае если средний балл его оценки собственных способностей был менее или равен 4,9,

средний уровень сформированности умений и навыков – в диапазоне 5-7,4 баллов, а высокий уровень – 7,5 баллов и более.

Исследование по данному показателю деятельностного критерия выявило, что в КГ 15,6 % обучающихся обладают фрагментарным уровнем сформированности умений и навыков, 75 % – средним и 9,4 % студентов имеют высокий уровень сформированности соответствующих умений и навыков. В ЭГ показатель низкого уровня – у 20,4 %, среднего – у 73,5 %, высокого – у 6,1 % студентов [2, с.97].

Результаты анкетирования показали, что уровень показателя деятельностного критерия в КГ и ЭГ примерно одинаковый и находится на *среднем уровне*.

С целью выявления уровня показателя **эмоционально-оценочного критерия** была использована методика, разработанная К.А. Филипповой [106, с. 172-179]. В соответствии с авторской методикой профессиональная и личностная компетентность исследуется с помощью профессионального личностного опросника.

Анкета представлена 50 вопросами, сгруппированными в 5 групп по 10 вопросов. В рамках нашего исследования уровня сформированности профессиональной и личностной компетентности обучающихся были отобраны три наиболее подходящие группы: «Представление о процессе обучения», «Профессиональная карьера» и «Я-реальное в будущем», соответствующие выделенными нами трем показателям эмоционально-оценочного критерия: представление о процессе обучения, видение перспектив профессионального и карьерного роста, уверенность в себе и в своей будущей профессиональной эффективности [2, с.98].

Результаты тестирования по каждой из трех групп обрабатывались отдельно и интерпретировались в соответствии с рекомендацией автора методики:

- суммарный балл более 70% характеризуется автором как сформированность учебно-профессиональной деятельности (высокий уровень);
- суммарный балл в диапазоне 50-70% – характеризуется как

оптимальный показатель (средний уровень);

– суммарный балл 49% и менее будет соответствовать низкому уровню по соответствующим показателям.

По первому показателю критерия «представление о процессе обучения» были получены следующие результаты.

Негативная направленность представлений о целях обучения в вузе, в целом недостаточная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента (низкий уровень) обнаружилась у 28,1 % студентов КГ и 16,3 % ЭГ. Нейтральная направленность (средний уровень) у 50,0 % КГ и 42,9 % ЭГ. Позитивная направленность представления о целях обучения в вузе, адекватная для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента (высокий уровень) по результатам тестирования соответствует 21,9 % КГ и 40,8 % обучающимся ЭГ [2, с.98].

Таким образом, обе группы по первому показателю эмоционально-оценочного критерия имеют *средний уровень* сформированности.

По второму исследуемому показателю «видение перспектив профессионального и карьерного роста» эмоционально-оценочного критерия были получены следующие результаты.

21,9% обучающихся КГ и 14,3% ЭГ имеют смутное представление о перспективах и планах относительно личной профессиональной карьеры, то есть в данном случае будем говорить о низком уровне сформированности показателя. Средний уровень (частичное видение перспектив и планов относительно личной профессиональной карьеры) демонстрируют 56,3% студентов КГ и 49,0% ЭГ. Высокий уровень, соответствующий четкому видению перспектив и выраженной способности планировать личную профессиональную карьеру, у 21,9% КГ и 36,7% ЭГ [2, с.98].

ЭГ и КГ по второму показателю эмоционально-оценочного критерия исходно имеют *средний уровень* сформированности.

Третий показатель эмоционально-оценочного критерия «уверенность в себе и в своей будущей профессиональной эффективности» диагностировался группой вопросов профессионального личностного опросника «Я-реальное в будущем» [2, с.98].

Профессиональное будущее представляют неопределенным и имеют низкий уровень сформированности показателя у 25,0 % КГ и 18,4 % ЭГ. Представление о своей будущей профессиональной эффективности в целом оптимистичны, но имеются сомнения (средний уровень) у 40,6% в КГ и 40,8% в ЭГ. Устойчивое оптимистическое представление о своей будущей профессиональной эффективности (высокий уровень) демонстрируют 34,4% в КГ и 40,8% в ЭГ [2, с.98]. Таким образом, обе группы по третьему показателю эмоционально-оценочного критерия исходно имеют *средний уровень* сформированности.

Обобщая результаты исследования на констатирующем этапе мотивационного, когнитивного, деятельностного и эмоционально-оценочного критериев, мы обнаружили следующие показатели уровня готовности студентов старших курсов к будущей профессиональной деятельности: низкий у 15,6% студентов КГ и 18,4% ЭГ; средний – у 68,8% КГ и 63,3% ЭГ; высокий – 15,6% КГ и 18,4% ЭГ (таблица 6).

Таблица 6 – Результаты оценки уровней готовности студентов к будущей профессиональной деятельности по критериям на констатирующем этапе

Критерии	Уровни	Результаты			
		КГ		ЭГ	
		Кол-во обучающихся	%	Кол-во обучающихся	%
Мотивационный	Низкий	7	21,9	6	12,2
	Средний	13	40,6	28	59,2
	Высокий	12	37,5	14	28,6
Когнитивный	Низкий	6	18,8	6	12,2
	Средний	22	68,8	36	75,5
	Высокий	4	12,5	6	12,2
Деятельностный	Низкий	5	15,6	10	20,4
	Средний	24	75,0	35	73,5
	Высокий	3	9,4	3	6,1
Эмоционально-оценочный	Низкий	8	25,0	11	22,4
	Средний	17	53,1	20	42,9
	Высокий	7	21,9	17	34,7

## Продолжение Таблицы 6

Критерии	Уровни сформированности	Показатели по группам			
		Контрольная группа		Контрольная группа	
		Количество человек	%	Количество человек	%
<b>Уровни готовности студентов к будущей профессиональной деятельности</b>					
	Низкий	5	15,6	9	18,4
	Средний	21	68,8	31	63,3
	Высокий	5	15,6	9	18,4

Графическая интерпретация полученных данных по мотивационному, когнитивному, деятельностному и эмоционально-оценочному критериям на констатирующем этапе представлена на рисунке 21.

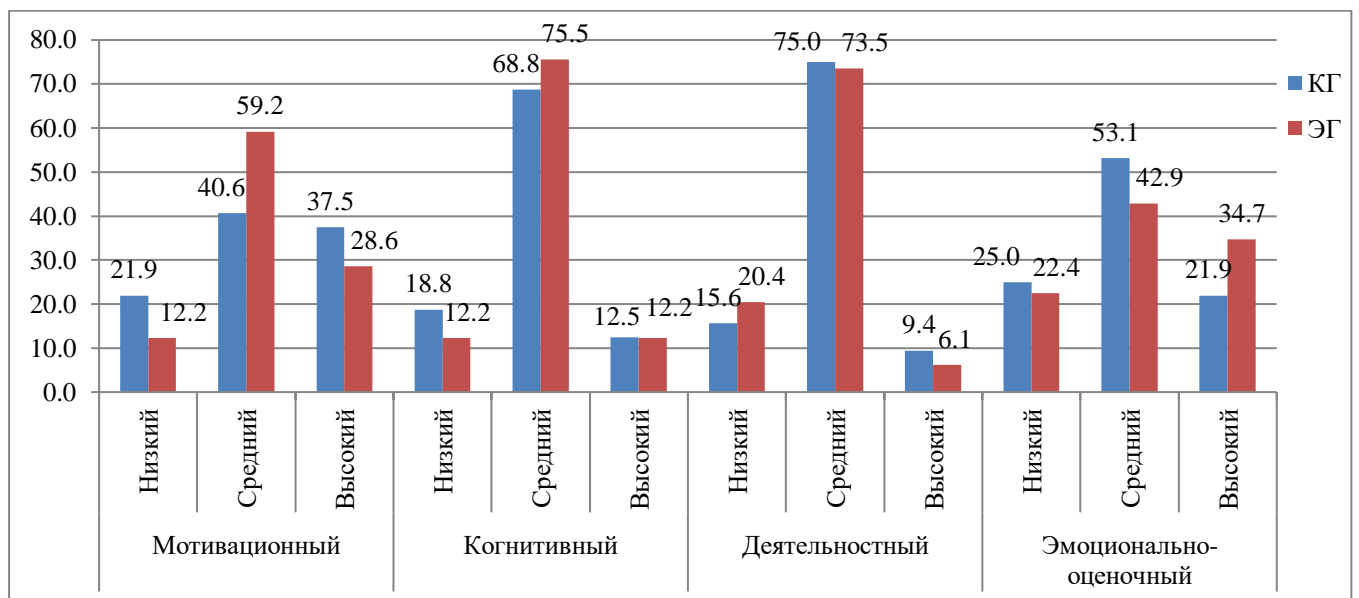


Рисунок 21– Результаты оценки уровня готовности студентов к будущей профессиональной деятельности по критериям на констатирующем этапе, %.

Таким образом, на констатирующем этапе распределение студентов по уровням готовности к будущей профессиональной деятельности примерно одинаковое в КГ и ЭГ с выраженным преобладанием среднего уровня.

*Контрольный этап опытно-экспериментальной работы*

Оценка достигнутого уровня готовности студентов к будущей профессиональной деятельности также осуществлялась с использованием показателей мотивационного, когнитивного, деятельностного и эмоционально-оценочного критериев. Для итоговой диагностики применялись методики, указанные в таблице 3.

Применение методики экспресс-диагностики личностной конкурентоспособности (Н.П. Фетискин) по окончании эксперимента показало, что в ЭГ существенно сократилось количество студентов с преобладанием свойств, препятствующих проявлению личностной конкурентоспособности – 4,1 % (на констатирующем этапе – 12,5 %). Незначительный уровень личностной конкурентоспособности продемонстрировали 51 % студентов. Средний уровень обнаружился у 42,9 % (на 12 % больше начального уровня). У одного студента был диагностирован высокий уровень личностной конкурентоспособности.

В КГ экспресс-диагностика выявила следующие показатели: 12,5 % – преобладание свойств, препятствующих проявлению личностной конкурентоспособности, 59,4 % обучающихся – незначительный, 28,1 % – средний уровень личностной конкурентоспособности.

Результаты исследования показывают, что, в целом, личностная конкурентоспособность в ЭГ повысилась.

С помощью методики для диагностики учебной мотивации студентов (А.А. Реан и В.А. Якунин, модификация Н.Ц. Бадмаевой) снова были исследованы два показателя мотивационного критерия: проявление интереса к профессиональной деятельности и проявление интереса к учебно-познавательной деятельности (таблица 7).

Напомним, что при первичном анализе результатов по данной методике, мы просчитывали, какое количество обучающихся высоко оценили данные мотивы по значимости, то есть средний балл по шкале был от 4,0 до 5,0 баллов.



Таблица 7 – Распределение мотивов по шкалам в КГ и ЭГ до и после проведения опытно-экспериментальной работы

Шкала мотивов	КГ		ЭГ	
	До %	После %	До %	После %
Коммуникативные	40,6	43,8	32,7	38,8
Избегания	9,4	12,5	8,2	10,2
Престижа	18,8	18,8	26,5	30,6
<b>Профессиональные</b>	<b>40,6</b>	<b>56,3</b>	<b>34,7</b>	<b>55,1</b>
Творческой самореализации	34,4	40,6	36,7	51,0
<b>Учебно-познавательные</b>	<b>28,1</b>	<b>28,1</b>	<b>30,6</b>	<b>49,0</b>
Социальные	21,9	21,9	28,6	21,9

Однако подобный анализ не дает нам полное представление об изменениях по профессиональным и учебно-познавательным мотивам, потому отдельно анализируем уровень сформированности по второму и третьему показателю. Оказалось, что в ЭГ больше не осталось студентов со слабо выраженной профессиональной мотивацией (на констатирующем этапе данный уровень обнаруживался у 24,5 %), ситуативную профессиональную мотивацию демонстрируют 22,4 %, а ярко выраженной мотивацией в профессиональной сфере обладают 77,6 % студентов ЭГ (ранее – 40,8 %) [2, с.96].

В КГ значимо данный показатель не изменился. Низкий уровень – у 12,5 % студентов (ранее 18,8 %), средний – 28,1 % (ранее 25,0 %) и высокий уровень – 59,4 % студентов (ранее 56,3 %).

Распределение по уровням третьего показателя (проявление интереса к учебно-познавательной деятельности) следующее: аналогично предыдущему показателю в ЭГ не осталось студентов с низкой мотивацией (до изучения вендорского курса низкий уровень был у 26,5 % студентов). Средний уровень сформированности по данному показателю имеют 26,5 % студентов, а высокий уровень увеличился в 2 раза – 73,5 % [2, с.96].

Уровень сформированности мотивационного критерия заметно повысился в ЭГ: высокий уровень после опытно-экспериментальной работы наблюдается у 73,5 % студентов (ранее – 28,6 %), а низкий уровень не обнаружился ни у одного студента ЭГ. В КГ значимых различий не наблюдается. На рисунке 22 показан

уровень мотивационного критерия до и после опытно-экспериментальной работы в КГ и ЭГ [2, с.96].

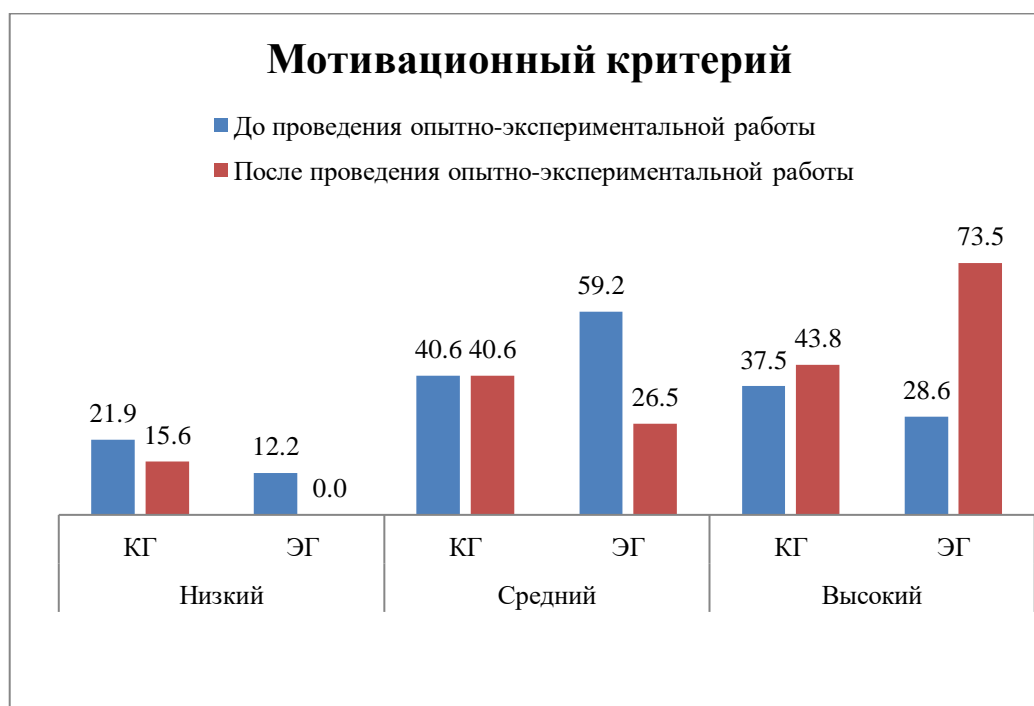


Рисунок 22 – Уровень развития мотивационного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.

Исследование динамики уровня развития мотивационного критерия обнаружило, что в КГ остался на прежнем *среднем уровне*, в ЭГ – поднялся до *высокого уровня*.

Уровень сформированности когнитивного критерия был проанализирован с помощью итогового тестирования вендорского курса Сетевой академии Cisco «Основы кибербезопасности», состоящего из 50 вопросов. Так как студенты КГ изучали аналогичные темы, что и студенты ЭГ мы сочли возможным провести одинаковую диагностику по данному критерию в обеих группах.

Результаты тестирования показали, что уровень развития когнитивного критерия после опытно-экспериментальной работы повысился в КГ и ЭГ [2, с.97] (рисунок 23).

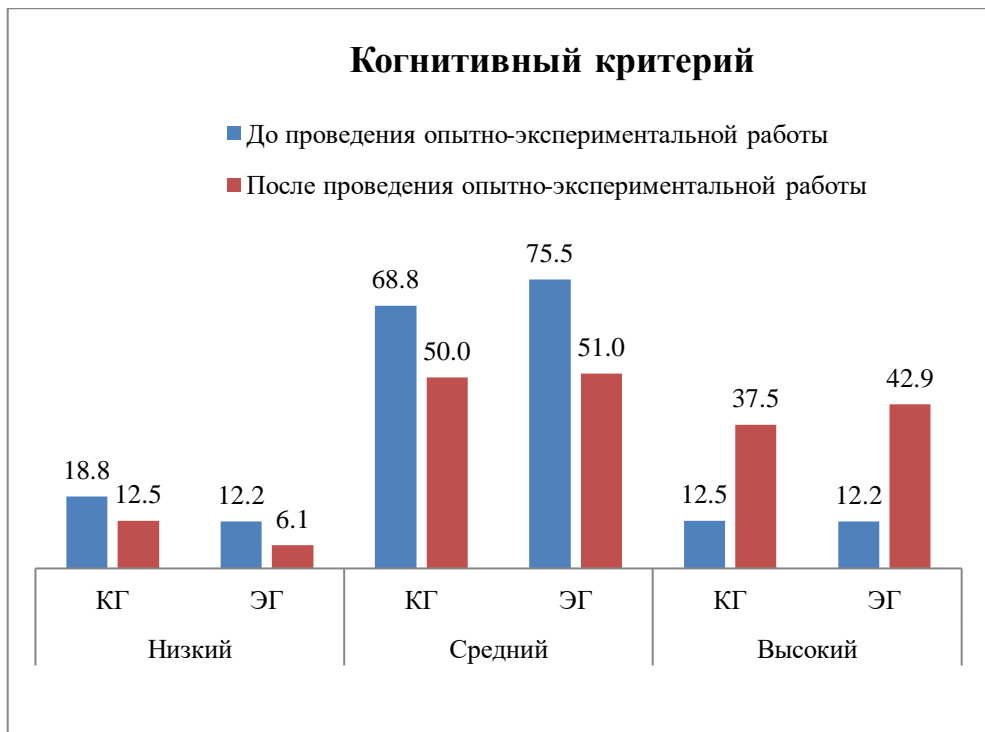


Рисунок 23 – Уровень развития когнитивного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.

Аналогичную картину можем наблюдать и по результатам самооценки студентов своих знаний и умений, характеризующим уровень развития деятельностного критерия. Результаты самооценки студентов умений и навыков в КГ и ЭГ до и после опытно-экспериментальной работы проиллюстрированы в таблице 8: средний балл самооценки по навыкам и умениям несколько повысился, причем повышение произошло равномерно и в КГ и в ЭГ [2, с.97].

Таблица 8 – Результат самооценки студентов умений и навыков в КГ и ЭГ до и после опытно-экспериментальной работы

	<b>Умения и навыки применения современных подходов к технологиям и методам обеспечения информационной безопасности</b>	<b>КГ</b>		<b>ЭГ</b>	
		До	После	До	После
1.	Навыки поиска вакансий в сфере информационной безопасности	5,3	6,4	5,2	5,9
2.	Умение оценить угрозы, исходящие от кибератак	5,9	6,4	5,9	6,4
3.	Навыки использования многофакторной аутентификации для защиты личной учетной записи	7,0	7,1	6,8	7,2
4.	Навыки исключения несанкционированного доступа к личной учетной записи и проверки активности учетной записи	7,3	7,3	7,3	7,6
5.	Навыки применения мер обеспечения безопасности на хостовой машине методом создания и проверки групп, пользователей и паролей	7,0	7,0	6,2	7,1
6.	Навыки применения мер обеспечения безопасности на хостовой машине методом назначения разрешений с использования символического и абсолютного обозначения	5,7	6,4	5,6	6,6
7.	Умение выявлять угрозы и уязвимости в системе с помощью средства для анализа топологии сетевой инфраструктуры (сканера портов)	5,5	6,4	5,8	6,3
8.	Умение применять методы стеганографии (сокрытия документа внутри графического файла )	5,1	6,2	5,1	5,9
9.	Умение выяснить пароль пользовательских учетных записей с помощью специальных утилит	5,6	6,6	5,8	6,5
10.	Навык использования цифровых подписей для подписания юридического документа	5,9	6,4	5,8	6,6
11.	Навык проверки электронного документа и цифровой подписи	5,9	6,3	6,1	6,9
12.	Умение создать собственную цифровую подпись	6,8	6,8	6,5	7,0
13.	Умение использовать протокол SSH для удаленного подключения к хосту	5,9	6,6	5,6	6,4
14.	Умение использовать протокол Telnet для удаленного подключения к хосту	6,2	6,6	5,6	6,6
15.	Умение использовать инструменты повышения надежности операционной системы	7,1	7,2	7,1	7,6
16.	Навык анализа примененных инструментов повышения надежности операционной системы и интерпретации предупреждений и рекомендаций системы	6,3	6,6	6,8	7,2

Графическое отображение динамики развития деятельностного критерия (рассчитанный средним баллом самооценки навыков и умений по каждому студенту) до и после эксперимента с процентными данными представлено на рисунке 24.

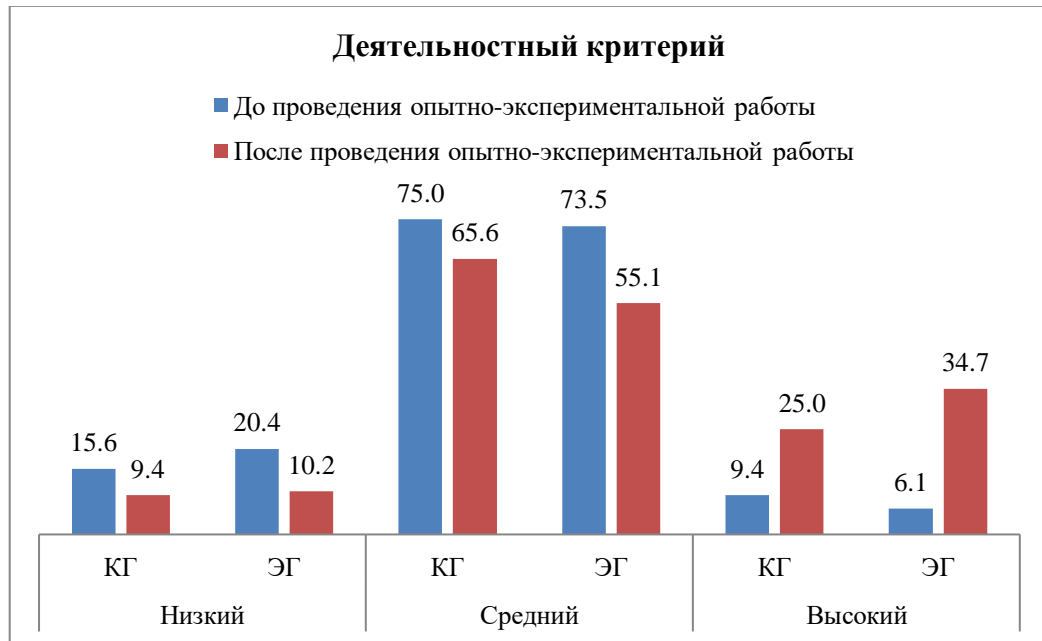


Рисунок 24 – Уровень развития деятельностного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.

Полученный результат по когнитивному и деятельностному критерию может объясняться тем, что студенты обеих групп изучали схожий теоретический материал и выполняли аналогичные практические и лабораторные работы, соответственно уровень теоретических знаний, а также умений и навыков повысился примерно одинаково и у студентов, изучающих вендорский курс, и у студентов, занимающихся с преподавателем традиционными методами [2, с.97].

Последняя методика диагностики – *профессиональный личностный опросник* – была применена с целью определения уровня сформированности трех показателей эмоционально-оценочного критерия.

Представление о процессе обучения является первым показателем критерия. По данному показателю в ЭГ получены следующие результаты тестирования: студентов с негативной направленностью представлений о целях обучения в вузе в группе не осталось (ранее – 16,3 %), 46,9 % обучающихся в ЭГ после

проведения опытно-экспериментальной работы имеют нейтральную направленность, а 53,1 % – позитивную направленность представления о целях обучения в вузе, адекватную для наполнения ценностно-смыслового содержания учебно-профессиональной деятельности студента [2, с.98].

В КГ значительных изменений по данному показателю не произошло. Негативную направленность имеют 25,0 % студентов (до проведения опытно-экспериментальной работы – 28,1 %), студентов с нейтральной направленностью, как и ранее – 50,0 %, а с позитивной – на 3,1 % больше и теперь составляет 25,0 %.

Таким образом, уровень сформированности по первому показателю эмоционально-оценочного критерия в ЭГ стал *высоким*, а уровень в КГ остался на прежнем *среднем* уровне.

Определение представления у студентов перспектив их профессионального и карьерного роста в ЭГ показало, что 69,4 % обучающихся ЭГ стали четко видеть перспективу и имеют выраженную способность планировать личную профессиональную карьеру. При этом один студент, по-прежнему, имеет смутное представление о перспективах и планах относительно своей карьеры. Количество студентов, которым характерно частичное видение перспектив и планов относительно личной профессиональной карьеры также заметно снизилось – до 28,6 % [2, с.98].

Ситуация в контрольной группе осталась аналогичной той, которая наблюдалась на констатирующем этапе проведения опытно-экспериментальной работы. Низкий уровень по данному показателю имеют 18,8 %, средний – 56,3 % и высокий – 25,0 % [2, с.98]. Следовательно, уровень по второму показателю изменился только в ЭГ, достигнув *высокого* значения.

По следующей шкале профессионального личностного опросника «Я-реальное в будущем» был определен уровень уверенности студентов в себе и в своей будущей профессиональной эффективности. В ЭГ больше не осталось студентов, которым профессиональное будущее представляется неопределенным. Абсолютное большинство, 75,5 % обучающихся, теперь имеют устойчивое

оптимистическое представление о своей будущей профессиональной эффективности. Одновременно с этим в КГ значимых изменений по данному показателю не наблюдалось [2, с.98].

Обобщая полученные результаты по всем показателям эмоционально-оценочного критерия, можно сделать вывод о том, что уровень значимо повысился в ЭГ [2, с.98]. На рисунке 25 представлена динамика уровня сформированности эмоционально-оценочного критерия до и после эксперимента.

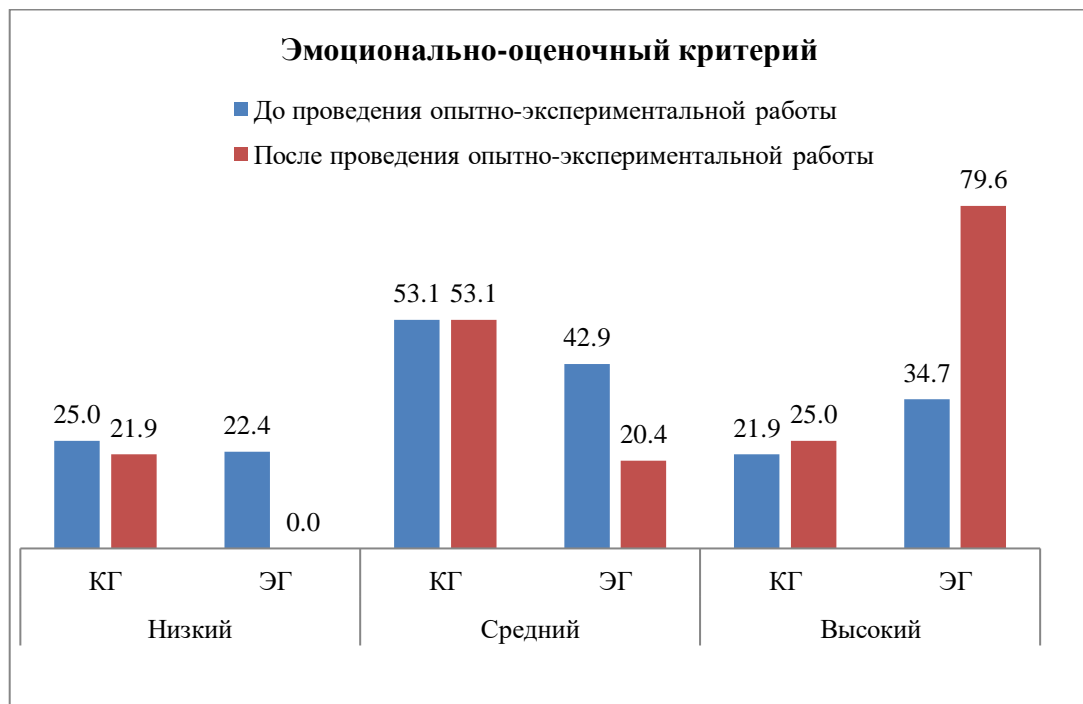


Рисунок 25 – Уровень развития эмоционально-оценочного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.

Уровень развития по мотивационному, когнитивному, деятельностному и эмоционально-оценочному критериям на констатирующем и контрольном этапе опытно-экспериментальной работы в обеих группах продемонстрирован в таблице 9.

Таблица 9 – Динамика уровня развития по мотивационному, когнитивному, деятельностному и эмоционально-оценочному критериям студентов в КГ и ЭГ (в %).

Уровни	г р у п п ы	Критерии							
		Мотивационный		Когнитивный		Деятельностный		Эмоционально-оценочный	
		До %	После %	До %	После %	До %	После %	До %	После %
Низкий	КГ	21,9	15,6	18,8	12,5	15,6	9,4	25,0	21,9
	ЭГ	12,2	0,0	12,2	6,1	20,4	10,2	22,4	0,0
Средний	КГ	40,6	40,6	68,8	50,0	75,0	65,6	53,1	53,1
	ЭГ	59,2	26,5	75,5	51,0	73,5	55,1	42,9	20,4
Высокий	КГ	37,5	43,8	12,5	37,5	9,4	25,0	21,9	25,0
	ЭГ	28,6	73,5	12,2	42,9	6,1	34,7	34,7	79,6

На заключительном этапе опытно-экспериментальной работы по внедрению вендорского образовательного курса изучался достигнутый уровень готовности студентов к будущей профессиональной деятельности в ЭГ и КГ. Итоговые результаты исследования представлены в таблице 10.

Таблица 10 – Итоговый уровень готовности студентов к будущей профессиональной деятельности в ЭГ и КГ после проведения опытно-экспериментальной работы

Уровни	Контрольная группа		Экспериментальная группа	
	Количество человек	%	Количество человек	%
Низкий	4	12,5	1	2,0
Средний	16	50	10	20,4
Высокий	12	37,5	38	77,6



Таким образом, в КГ в начале и по окончании опытно-экспериментальной работы произошли следующие изменения в распределении студентов. В начале опытно-экспериментальной работы у 15,6 % обучающихся был выявлен низкий уровень готовности к профессиональной деятельности, а в конце этот показатель составил 12,5 %. Средний уровень в начале имели 68,8 % студентов и 15,6 % высокий уровень готовности к профессиональной деятельности, по завершении опытно-экспериментальной работы результаты по данным показателям составили 50,0 % и 37,5 % соответственно [2, с.99].

Значительное повышение количества студентов, имеющих высокий уровень готовности, произошло за счет увеличения уровня по показателям когнитивного и деятельностного критериев. Это объясняется тем, что, как уже было сказано выше, студенты КГ изучали темы и выполняли практические и лабораторные работы, аналогичные тем, которые были включены в вендорский учебный курс [2, с.99].

Одновременно с этим, существенных изменений по мотивационному и эмоционально-оценочному критериям не произошло [2, с.99].

Изменение ситуации в экспериментальной и контрольной группе в начале и в конце опытно-экспериментальной работы наглядно представлено на рисунке 26.

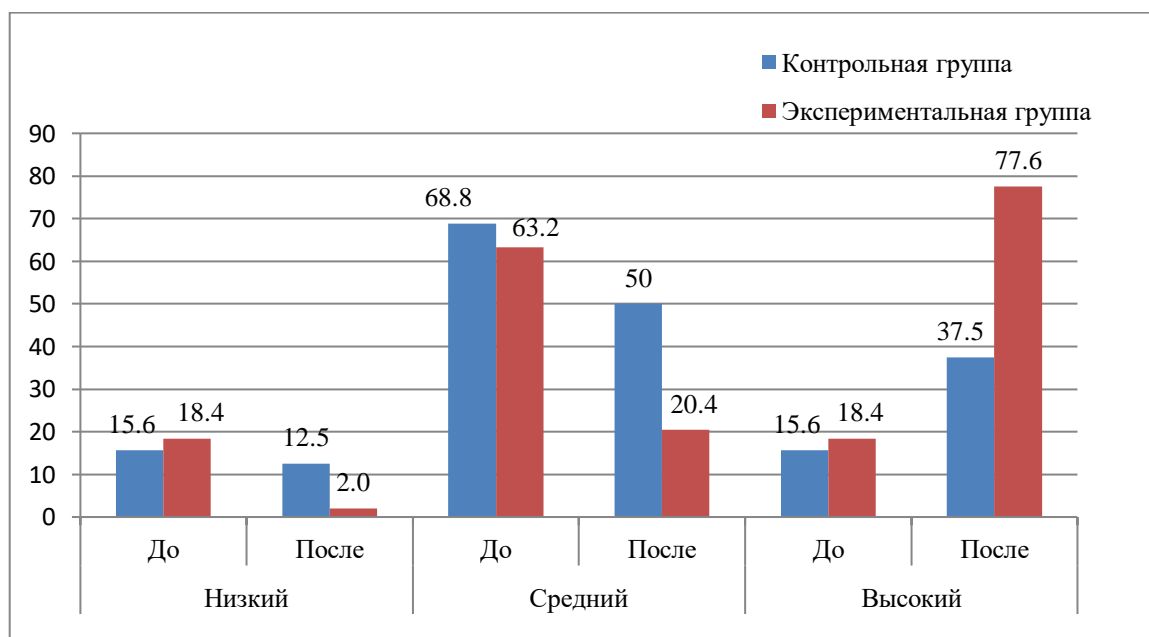


Рисунок 26 – Итоговое сравнение результатов общего уровня готовности студентов к будущей профессиональной деятельности, %.

На диаграмме видно, что произошли значительные изменения в ЭГ, прежде всего в том, что существенно выросло количество студентов, обладающих высоким уровнем готовности к будущей профессиональной деятельности. На начальном этапе таких студентов было 18,4 %, по окончании опытно-экспериментальной работы – 77,6 %. Низким уровнем готовности отличился один студент, что составляет 2 %.

Интерпретируя полученные результаты по критериям готовности к будущей профессиональной деятельности можно сделать вывод о том, что различия между КГ И ЭГ проявляются только по мотивационному и эмоционально-оценочному критериям. Следовательно, изучение вендорского учебного курса студентами повышает интерес к учебно-познавательной и профессиональной деятельности, позволяют студенту – будущему специалисту по информационной безопасности – увидеть перспективы в своем профессиональном росте и осознать собственную профессиональную эффективность [2, с.100].

Мы видим причину подобных позитивных изменений в том, что студент, изучая курс популярной и авторитетной отечественной или зарубежной ИТ-компании, как бы выходит за рамки образовательной среды вуза и интегрируется в общемировое профессиональное сообщество. Это убеждает будущего специалиста в области информационной безопасности в актуальности и значимости своих сформированных способностей и дает ему возможность иметь оптимистическое представление о своей будущей профессиональной деятельности [2, с.100].

#### *Обоснование полученных результатов методом математической статистики*

Проведем статистическую проверку полученных результатов полученных результатов после проведения опытно-экспериментальной работы. Все расчеты будем производить с использованием программы для статистической обработки данных IBM SPSS Statistics.

С помощью непараметрического U-критерия Манна-Уитни для независимых выборок проверялась статистическая гипотеза о равенстве средних

значений в КГ и ЭГ до и после проведения опытно-экспериментальной работы. Проверка проводилась для каждого критерия (мотивационный, когнитивный, деятельностный и эмоционально-оценочный) и общего уровня готовности студентов к будущей профессиональной деятельности. Данные проверки гипотез представлены в сводной Таблице 11, где  $x_1$  и  $x_2$  – среднее значение выборки КГ и ЭГ соответственно,  $U$  –  $U$ -критерий Манна-Уитни для независимых выборок,  $p$  – асимптотическая значимость (2-сторонний критерий) [2, с.99].

Детальные сведения расчета  $U$ -критерия Манна-Уитни в IBM SPSS Statistics представлены в приложении Т.

Таблица 11 – Результаты статистической обработки данных до и после проведения опытно-экспериментальной работы

Критерии	$\bar{x}_1$	$\bar{x}_2$	$U$	$p$	Вывод
<b>До проведения опытно-экспериментальной работы</b>					
Мотивационный	1,156	1,163	791,500	0,936	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
Когнитивный	0,937	1,000	741,000	0,594	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
Деятельностный	0,938	0,857	839,500	0,484	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
Эмоционально-оценочный	0,969	1,122	693,000	0,343	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
<b>Уровень готовности студентов к будущей проф. деятельности</b>	4,000	4,143	712,500	0,480	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
<b>После проведения опытно-экспериментальной работы</b>					
Мотивационный	1,281	1,734	518,500	0,003	$p \leq 0,01$ , следовательно, различия обнаружены на высоком уровне статистической значимости
Когнитивный	1,250	1,367	716,000	0,463	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
Деятельностный	1,156	1,244	720,000	0,479	$p > 0,1$ , следовательно, статистически достоверные различия не обнаружены
Эмоционально-оценочный	1,031	1,796	321,000	0,000	$p \leq 0,01$ , следовательно, различия обнаружены на высоком уровне статистической значимости

Продолжение Таблицы 11

Критерии	$\bar{x}_1$	$\bar{x}_2$	U	p	Вывод
Уровень готовности студентов к будущей проф. деятельности	4,719	6,143	362,500	0,000	$p \leq 0,01$ , следовательно, различия обнаружены на высоком уровне статистической значимости

Анализ данных таблицы 11 позволяет заключить:

– студенты ЭГ и КГ до проведения опытно-экспериментальной работы имели примерно одинаковый уровень готовности к будущей профессиональной деятельности (по данным выборкам статистически достоверные различия не обнаружены);

– повышение уровня развития по когнитивному и деятельностному критериям в ЭГ и КГ после проведения опытно-экспериментальной работы произошло примерно в равной степени (по данным выборкам статистически достоверные различия не обнаружены);

– имеются значимые различия по уровням развития мотивационного и эмоционально-оценочного критериев, а также по общему уровню готовности студентов к будущей профессиональной деятельности после проведения опытно-экспериментальной работы между КГ и ЭГ (различия обнаружены на высоком уровне статистической значимости) [2, с.99].

С помощью непараметрического критерия знаковых рангов Уилкоксона для связанных выборок проверялась статистическая гипотеза о равенстве средних значений в ЭГ до и после проведения опытно-экспериментальной работы. Статистика критерия знаковых рангов Уилкоксона между указанными выборками составила – 1035,000, асимптотическая значимость (2-сторонний критерий) – 0,000, следовательно, различия обнаружены на высоком уровне статистической значимости.

Детальные сведения расчета критерия Уилкоксона в IBM SPSS Statistics представлены в приложении У.

Таким образом, по окончании апробирования внедрения вендорского учебного курса уровень готовности студентов к будущей профессиональной

деятельности в ЭГ вырос, что следует из результатов диагностики, полученных в начале и конце опытно-экспериментальной работы.

## ВЫВОДЫ ПО ГЛАВЕ 2

Во 2-й главе проанализировано становление отечественного и зарубежного профессионального образования по защите информации в рамках историко-логического подхода и определены следующие этапы развития системы профессионального образования специалистов по информационной безопасности в России:

- этап подготовки кадров, способных решать фрагментарные вопросы защиты информации в «закрытых» ведомственных учреждениях (до 1940х гг.);
- этап подготовки специалистов по информационной безопасности в учреждениях высшего образования по «закрытым» программам (1940-е-1984 гг.);
- этап появления отдельных «открытых» образовательных программ по информационной безопасности в учреждениях высшего образования (1985-конец 1990-х гг.);
- этап массовой реализации программ по информационной безопасности в образовательных учреждениях разного уровня (2000-2010 гг.);
- этап подготовки специалистов по информационной безопасности по сферам деятельности (с 2010 г. по настоящее время).

Этапы становления системы профессионального образования специалистов по защите информации были выделены и анализированы в контексте формирования мировой информационно-коммуникационной среды и развития методов обеспечения информационной безопасности. Проанализированы некоторые исторические аспекты становления систем обеспечения безопасности данных в зарубежных государствах и их воздействие на развитие системы профессиональной подготовки специалистов по защите информации. Обнаружены отдельные соответствия в становлении государственной системы защиты информации и содержания профессиональной подготовки специалистов в данной области (например, популярность образовательных программ в США по расследованию компьютерных инцидентов, «усиленный» блок юридических

дисциплин в Великобритании, нацеленность на изучение криптографических методов защиты информации во Франции).

На основе системного подхода были определены критерии сопоставления систем профессионального образования будущих специалистов по информационной безопасности в России и за рубежом: цель подготовки будущих специалистов (как системообразующий фактор), направления подготовки и профили, содержание образования (содержательная подсистема), образовательные организации, образовательные технологии, профессорско-преподавательский состав (функциональная подсистема), управление содержанием образовательных программ, сложившиеся ступени подготовки (организационно-управленческая подсистема).

Обнаружены общие черты и ключевые различия в российской, британской, американской, немецкой и французской системах профессиональной подготовки специалистов по защите информации.

Показано, что профессиональное образование в данной области строится на схожей целевой основе (формирование у будущих выпускников компетенций, необходимых для квалифицированного решения задач обеспечения информационной безопасности в условиях существования угроз). Профессиональное образование будущих специалистов по информационной безопасности осуществляется в образовательных организациях среднего, высшего и дополнительного образования (с учетом особенностей государственных систем профессионального образования). В каждом рассмотренном государстве подготовкой кадров по обеспечению информационной безопасности занимаются преподаватели, имеющие ученую степень, базовое высшее образование, а также ведущие специалисты со стороны профессионального сообщества.

Найдены ключевые различия профессионального образования специалистов по информационной безопасности в России и зарубежных странах (США, Великобритания, Франция, Германия). По организационно-управленческой подсистеме были выделены ключевые различия по управлению содержанием образовательных программ и по ступеням подготовки. Различие в управлении

содержанием образовательных программ заключается, прежде всего, в частичном управлении содержанием и требований к выпускникам профильными министерствами, а также органами государственной власти, регулируемыми вопросы защиты информации. В зарубежных странах образовательные организации, в основном, регулируют содержание самостоятельно, опираясь на социальный заказ и рынок трудоустройства выпускников, требования к профессиональной сертификации специалистов.

Только в России допускается моноуровневый маршрут, вследствие сохранения традиционного для нашей страны уровня специалитета, при параллельной возможности обучаться по программам многоуровневого маршрута – бакалавриата и магистратуры. В зарубежных странах подготовка будущих специалистов по информационной безопасности осуществляется только в рамках многоуровневой модели.

По критериям сопоставления функциональной подсистемы были выделены ключевые различия по отдельным образовательным технологиям, которые заключаются в формах организации учебного процесса, способах промежуточной и итоговой аттестации. Для отечественных образовательных программ характерны лекции, практические и лабораторные работы, семинары. В зарубежных образовательных программах, помимо традиционных лекций и семинаров, практическое обучение часто строится на выполнение проектов в небольших группах (обычно по 2-5 студентов), распространено привлечение специалистов из внешнего профессионального сообщества с целью разбора конкретных задач, кейсов и решения актуальных проблем.

Производственные практики, стажировки, а также реализуемые в процессе обучения проекты в рамках зарубежных образовательных программ по информационной безопасности ориентированы на рынок трудоустройства выпускников, чаще всего в бизнес-структурах (в большинстве случаев именно бизнес задает цель и содержание практики).

Отмечено, что ключевые различия, в первую очередь, выделяются по критериям содержательной подсистемы (направления подготовки и профили,



содержание образования).

В странах, для которых характерна распространенность образовательных программ по информационной безопасности (Россия, США, Великобритания) реализуется подготовка по всем выделенным укрупненным блокам. При этом в Германии мы не обнаружили отдельных программ по безопасности компьютерных сетей, расследованию компьютерных инцидентов и по криптографии. Образовательных программ, входящих в блок по законодательству в сфере информационной безопасности, не было выявлено во Франции. Вместе с тем, система профессионального образования специалистов по информационной безопасности во Франции значительное внимание уделяет аспектам криптографической защиты информации и математическим циклом образования. Отличительной национальной особенностью Великобритании является существование подготовки магистров в области права, связанной с законодательными аспектами информационной безопасности.

Следующим ключевым различием содержательной компоненты является присутствие комбинированных образовательных программ, фактически включающих в себя несколько профилей: «Управление рисками и информационная безопасность», «Информационная безопасность и биометрика», «Компьютерная экспертиза и компьютерная безопасность», «Информационная безопасность и компьютерные сети» и других «смешанных» образовательных программ в США и Великобритании.

Таким образом, можно сделать основные выводы по содержательной подсистеме:

– Совокупность дисциплин, входящих в образовательные программы блока, отличаются во всех рассматриваемых странах, что, вероятно, обусловлено социальным заказом профессионального сообщества, а также наличием или отсутствием управления содержанием образовательных программ.

– В большинстве зарубежных образовательных программах нами не было обнаружено дисциплин по изучению инженерно-технических методов

обеспечения информационной безопасности, обязательных для образовательных программ по информационной безопасности в отечественных вузах.

– В большинстве зарубежных образовательных программах нами не было обнаружено гуманитарных дисциплин, обязательных по отечественным образовательным стандартам или включенных дополнительно образовательными организациями России.

– В большинстве зарубежных образовательных программах присутствуют в значительном объеме дисциплины по компьютерной экспертизе и расследованию цифровых преступлений, которые на данный момент не получили широкого распространения в отечественных образовательных программах.

– В зарубежных образовательных программах широко распространены дисциплины экономического блока (менеджмент, управление бизнес-процессами и прочие);

– Большинство зарубежных образовательных программ интегрировано с вендорскими образовательными курсами и содержательно ориентируются на будущую вендорнезависимую сертификацию выпускников.

Обоснована возможность модернизации содержательной составляющей отечественной системы профессионального образования специалистов, выделены компоненты модернизации и механизмы их реализации:

– Переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества. Механизмом переориентации может стать включение в образовательные программы дисциплин (модулей), связанных с обеспечением информационной безопасности в бизнес-структурах и расширение сотрудничества образовательных организаций с бизнесом.

– Фрагментарное изменение содержания образовательных программ при помощи механизма включения дисциплин по компьютерной экспертизе,

расследованию цифровых преступлений и правоприменительными технологиями в сфере защиты информации.

– Интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров на основе механизма взаимодействия с ИТ-компаниями и включения вендорских и иных образовательных курсов в соответствующие программы дисциплин с возможной итоговой сертификацией.

Представлены результаты опытно-экспериментальной работы по интеграции образовательных программ с вендорским учебным курсом, которые показали, что уровень готовности студентов к будущей профессиональной деятельности после изучения вендорского учебного курса и получения соответствующего сертификата существенно повысился, прежде всего, за счет повышения уровня мотивационного и эмоционально-оценочного критериев. Соответственно, можно сделать вывод о том, что изучение вендорского учебного курса студентами, обучающимся по направлениям подготовки и специальностям в области информационной безопасности, повышает интерес к учебно-познавательной и профессиональной деятельности, позволяют студенту – будущему специалисту по информационной безопасности – увидеть перспективы в своем профессиональном росте и осознать собственную профессиональную эффективность.

## ЗАКЛЮЧЕНИЕ

Проведенный в диссертационной работе сравнительно-сопоставительный анализ систем профессионального образования в области информационной безопасности позволил сформулировать следующие основные выводы, подтверждающие правомерность выдвинутой гипотезы и решение поставленных в исследовании задач.

Проведение сравнительно-сопоставительного анализа целесообразно по следующим критериям сопоставления систем профессионального образования будущих специалистов по информационной безопасности в России и за рубежом: цель подготовки будущих специалистов (как системообразующий фактор), направления подготовки и профили, содержание образования (содержательная подсистема), образовательные организации, образовательные технологии, профессорско-преподавательский состав, целевая аудитория (функциональная подсистема), управление содержанием образовательных программ, сложившиеся ступени подготовки (организационно-управленческая подсистема).

Установлено, что системы профессионального образования будущих специалистов по информационной безопасности в России, США, Великобритании, Германии и Франции имеют общие черты и ключевые различия.

Системы профессионального образования специалистов по информационной безопасности в рассматриваемых странах строятся на схожей целевой основе (в каждой стране ведется обучение специалистов, способных решать задачи обеспечения информационной безопасности в условиях существования угроз в информационной сфере). Профессиональное образование будущих специалистов по информационной безопасности осуществляется в образовательных организациях среднего, высшего и дополнительного образования (с учетом особенностей государственных систем профессионального образования). В каждом рассмотренном государстве подготовкой кадров по обеспечению информационной безопасности занимаются преподаватели,

имеющие ученую степень, базовое высшее образование, а также ведущие специалисты со стороны профессионального сообщества.

Системы профессионального образования специалистов по информационной безопасности в России, Великобритании, Германии, Франции и США имеют ряд особенностей. Ключевые различия, в первую очередь, выделяются по критериям содержательной подсистемы (направления подготовки и профили, содержание образования) и заключаются в следующем.

В большинстве американских, британских, немецких и французских образовательных программах по информационной безопасности отсутствуют дисциплины (модули, темы), связанные с методами технической (инженерно-технической) защиты информации, распространенные в отечественных образовательных программах. Также отсутствуют гуманитарные дисциплины (философия, история и другие), обязательные по отечественным образовательным стандартам или включенные дополнительно образовательными организациями России. Вместе с тем в большинстве зарубежных образовательных программах присутствуют в значительном объеме дисциплины по компьютерной экспертизе и расследованию цифровых преступлений, которые на данный момент не получили широкого распространения в отечественных образовательных программах. За рубежом широко распространены дисциплины экономического блока (менеджмент, управление бизнес-процессами и прочие).

Набор образовательных программ, входящих в укрупненные блоки направлений подготовки и специальностей, различен для всех рассматриваемых стран. Набор дисциплин, входящих в схожие образовательные программы специалистов по информационной безопасности также различен для всех рассматриваемых стран.

В Великобритании присутствуют образовательные программы по направлениям подготовки, связанным с правовыми аспектами информационной безопасности при получении соответствующей степени (магистр права). В образовательных программах Франции широко распространены дисциплины

(темы, модули) по криптографическим методам защиты информации и математическим циклом образования.

Ряд особенностей, выявленных по критериям функциональной и организационно-управленческой подсистем не являются специфичными для области профессионального образования будущих специалистов по информационной безопасности и, в большей степени, отражают особенности национальных систем профессионального образования (в ступенях подготовки, в управлении формированием образовательных программ, в образовательных технологиях, в ориентированности студенческих практик и стажировок на бизнес-структуры).

Сравнительный анализ российских и зарубежных систем подготовки будущих специалистов по информационной безопасности позволил обосновать возможность модернизации содержательной части отечественной системы профессионального образования специалистов с учетом позитивного зарубежного опыта. Выделены компоненты модернизации и механизмы их реализации:

1) Переориентация профессиональной подготовки в области информационной безопасности (по «открытым» образовательным программам) от потребностей, в большей степени, государственных органов на потребности, в том числе, «открытого» бизнес-сообщества. Механизмом переориентации может стать включение в образовательные программы дисциплин (модулей), связанных с обеспечением информационной безопасности в бизнес-структурах и расширение сотрудничества образовательных организаций с бизнесом.

2) Фрагментарное изменение содержания образовательных программ при помощи механизма включения дисциплин по компьютерной экспертизе, расследованию цифровых преступлений и правоприменительными технологиями в сфере защиты информации.

3) Интеграция образовательных программ с дополнительными образовательными курсами отечественных и зарубежных вендоров на основе механизма взаимодействия с ИТ-компаниями и включения вендорских и иных

образовательных курсов в соответствующие программы дисциплин с возможной итоговой сертификацией.

В ходе исследования было доказано, что включение вендорского образовательного курса с последующей сертификацией в образовательные программы по информационной безопасности обеспечивает повышение уровня готовности студентов к будущей профессиональной деятельности.

Сохранение национальной специфики подготовки будущих специалистов по информационной безопасности при одновременном переносе позитивного зарубежного опыта на отечественную систему образования в данной области позволит удовлетворить потребности в защите информационной сферы.

Перспективы разработки темы заключаются в дальнейшем изучении возможности переноса позитивного зарубежного опыта на отечественную систему образования специалистов в области информационной безопасности. Также перспективными направлениями видятся исследования в области эффективности внедрения других образовательных ресурсов отечественных и зарубежных вендоров и их комплексов в образовательные программы по информационной безопасности, а также исследования, связанные с вендорнезависимой профессиональной сертификации при подготовке специалистов по защите информации. Кроме того, по выделенным критериям сопоставления систем профессионального образования будущих специалистов по информационной безопасности возможно проведение сравнительно-сопоставительного анализа подготовки кадров по близким направлениям.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Аверченков, В.И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2007. – 223 с.
2. Анурьева, М.С. Влияние вендорских курсов на готовность студентов к будущей профессиональной деятельности / М.С. Анурьева // Профессиональное образование в России и за рубежом. – 2021. – № 4 (44). – С. 93-101.
3. Анурьева, М.С. Историко-логический анализ становления системы профессионального образования специалистов по защите информации / М.С. Анурьева // Профессиональное образование в России и за рубежом. – 2018. – № 2 (30). – С. 57-67.
4. Анурьева, М.С. Направления развития отечественной системы подготовки специалистов по защите информации / М.С. Анурьева // Вестник Тамбовского Университета. Серия: Естественные и технические науки. – 2013. – Т. 18. № 1. – С. 230-232.
5. Анурьева, М.С. Научный базис сравнительного анализа программ подготовки специалистов по информационной безопасности в разных странах / М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2018. – Т. 23. № 171. – С. 90-97.
6. Анурьева, М.С. О приоритетах образовательных программ в области информационной безопасности в разных странах / М.С. Анурьева // Психолого-педагогический журнал Гаудеамус. – 2013. – №1. – С.102-109.
7. Анурьева, М.С. Образовательные программы в области информационной безопасности в РФ / М.С. Анурьева // Актуальные проблемы информатики и информационных технологий: сборник материалов международной научно-практической конференции. – Тамбов: ТГУ имени Г.Р. Державина, 2017. – С. 13-20.



8. Анурьева, М.С. Общее и особенное в подготовке специалистов в области информационной безопасности России и за рубежом / М.С. Анурьева // Психолого-педагогический журнал Гаудеамус.– 2012. –№2. – С.116–118.
9. Анурьева, М.С. Опыт подготовки бакалавров по компьютерной экспертизе за рубежом / М.С. Анурьева // Компьютерные науки и информационные технологии: сборник материалов Международной научной конференции / ответственные за выпуск: Т.В. Семенова, А.Г. Федорова. – Саратов: ИЦ «Наука», 2016. – С. 54-56.
10. Анурьева, М.С. Подготовка бакалавров по компьютерной безопасности за рубежом / М.С. Анурьева // Преподавание информационных технологий в РФ: сборник материалов XIV открытой всероссийской конференции / Отв. ред. Альминдеров А.В., 2016 – С. 114-115.
11. Анурьева, М.С. Подготовка специалистов в области информационной безопасности: международный опыт / М.С. Анурьева // Преподавание информационных технологий в РФ: сборник материалов XI открытой Всероссийской конференции – Воронеж: Воронежский государственный университет, 2013.– С. 256-258.
12. Анурьева, М.С. Подготовка специалистов по расследованию цифровых преступлений в России и зарубежных странах / М.С. Анурьева // Образование и право. – 2021. – № 10. – С. 334–338.
13. Анурьева, М.С. Подходы к обучению по дисциплине «Расследование компьютерных инцидентов» в зарубежных странах / М. С. Анурьева // Психолого-педагогический журнал Гаудеамус. – 2013. – № 2(22). – С. 39-41.
14. Анурьева, М.С. Подходы к формированию содержания дисциплин по правовой защите информации за рубежом / М.С. Анурьева // Психолого-педагогический журнал Гаудеамус. – 2014. – № 2(24). – С. 124-129.
15. Анурьева, М.С. Система образования в области информационной безопасности в Великобритании / М.С. Анурьева, М.С. Чванова // Преподавание информационных технологий в РФ: сборник материалов IX Всероссийской конференции. – Саратов: ООО «Издательский Центр «Наука»», 2011. – С. 67-70.

16. Анурьева, М.С. Современная система образования в области информационной безопасности в РФ / М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2018. – Т. 23. № 173. – С. 111-120.
17. Анурьева, М.С. Сравнительный анализ системы высшего образования в области информационной безопасности в России и Германии / М.С. Анурьева // Информационные технологии в образовании: сборник материалов III Всероссийской научно-практической конференции. – Саратов: ООО «Издательский Центр «Наука»», 2011. – С. 80-82.
18. Архангельский, С.И. Некоторые методологические вопросы введения в теорию обучения высшей школы / С.И. Архангельский // Вопросы повышения эффективности теоретических исследований в педагогической науке. – В 2-х ч. – Ч. II. – М.: Знание, 1976. – 218 с.
19. Архангельский, С.И. Учебный процесс в высшей школе и его закономерные основы и методы: учеб.-метод. пособие / С.И. Архангельский – М.: Высшая школа, 1980. – 368 с.
20. Бадмаева, Н.Ц. Влияние мотивационного фактора на развитие умственных способностей / Н.Ц. Бадмаева; Федер. агентство по образованию, Восточно-Сибирское гос. технол. ун-т. – Улан-Удэ: Изд-во ВСГТУ, 2005. – С.151-154.
21. Башкиров, А.Н. Кибербезопасность инфраструктуры Германии // Зарубежное военное обозрение. – 2020. – №9. – С. 10-16.
22. Белов, Е.Б. Проекты квалификаций на основе профессиональных стандартов в области информационной безопасности [Электронный ресурс] / Е.Б. Белов, В.А. Шапошников. – URL: [http://azi.ru/wp-content/uploads/2018/04/BELOV\\_SHAPOSHNIKOV\\_VII\\_forum-AZI.pdf](http://azi.ru/wp-content/uploads/2018/04/BELOV_SHAPOSHNIKOV_VII_forum-AZI.pdf) (дата обращения 10.12.2018).
23. Белов, Е.Б. Траектории образования в области информационной безопасности/ Е.Б. Белов // Информационная безопасность. – 2007. – №6. – С.32-33.

24. Вагина, И.В. Сравнительный анализ систем среднего профессионального образования России и Франции: дис. ... канд. пед. наук: 13.00.08 / Вагина Ирина Валерьевна. – Шуя, 2011. – 182 с.
25. Воскресенская, Н.М. Некоторые вопросы методологии сравнительной педагогики в Англии в 80-х годах: концепция Б. Холмза // Методологические проблемы сравнительной педагогики. – М., 1991. – С. 51-70.
26. Вульфсон, Б.Л. Сравнительная педагогика: актуальные вопросы теории и методологии // Отечественная и зарубежная педагогика. – 2011. – №1. – С. 117-130.
27. Вульфсон, Б.Л. Сравнительная педагогика: учебное пособие / Б.Л. Вульфсон, З.А. Малькова. – М.; Воронеж: МОДЭК, 1996. – 256 с.
28. Германская служба академических обменов [Электронный ресурс]. – URL: <https://www.daad.ru/ru/> (дата обращения: 28.05.2018).
29. Гершунский, Б.С. Философия образования для XXI века. М.: Совершенство, 1998. – 608 с.
30. Грасс, Т.П. Взаимодействие школы и бизнеса как способ формирования экономической культуры у старшеклассников в России и зарубежных странах / Т.П. Грасс, В.И. Петрищев, Е.В. Рыбакова // Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокинетика. – 2019. – Т. 25. № 4. – С. 245-249.
31. Гриняев, С. Н. Информационная война: история, день сегодняшний и перспектива / С.Н. Гриняев. – Санкт-Петербург: Издательская группа «Арлит», 2000. – 240 с.
32. Гриняев, С.Н. Поле битвы - киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев. – Минск: Харвест, 2004. – 448 с.
33. Джурицкий, А.Н. Высшее образование в современном мире: тренды и проблемы: монографические исследования: педагогика / А.Н. Джурицкий – М.: Прометей, 2017. – 186 с.
34. Джурицкий, А.Н. Теория и методология истории педагогики и

- сравнительной педагогики. Актуальные проблемы: монографические исследования: педагогика / А.Н. Джуринский – М.: Прометей, 2014 – 130 с.
35. Дубова, Н.А. Зачем нужен CISSP [Электронный ресурс] / Н.А. Дубова // Директор информационной службы. – 2003. – № 09. URL: <https://www.osp.ru/cio/2003/09/172877/> (дата обращения: 28.11.2018)
36. Зуева, О.Н. Сравнительный анализ профессионального образования России и Венгрии: дис. ... канд. пед. наук: 13.00.08 / Зуева Ольга Николаевна. – Шуя, 2010. – 169 с.
37. Информация по образовательным программам, опубликованная на официальном сайте ФГБОУ ВО «ТГУ имени Г.Р.Державина». – [Электронный ресурс]. – URL: <https://www.tsutmb.ru/sveden/education/> (дата обращения 10.11.2021)
38. Исмаилов, Э.Э. Сравнительно-педагогический анализ систем среднего профессионального образования Швеции и России: дис. ... д-ра. пед.наук: 13.00.08 / Исмаилов Эльхан Эюб оглы. – Калининград, 2004. – 241 с.
39. ИТ-кадры для цифровой экономики в России. Ассоциация предприятий компьютерных и информационных технологий. – [Электронный ресурс]. – URL: [https://apkit.ru/files/it-personnel%20research\\_2024\\_АРКИТ.pdf](https://apkit.ru/files/it-personnel%20research_2024_АРКИТ.pdf) (дата обращения 10.11.2021).
40. Как получить CISA? [Электронный ресурс]. – URL: <https://isaca.ru/isaca-all-ru/cisa/cisa-howto-ru.html/> (дата обращения 10.11.2021).
41. Как получить CISM? [Электронный ресурс]. – URL: <https://isaca.ru/isaca-all-ru/cism-ru/cism-howto-ru.html/> (дата обращения 10.09.2021).
42. Камалеева, А.Р. Системный подход в педагогике / А.Р. Камалеева // Научно-педагогическое обозрение . – 2015. – №3 (9). – С.13-23.
43. Касперская, Н.И. Как России сохранить цифровой суверенитет [Электронный ресурс] / Н.И. Касперская // Российская газета. – № 54 (7517). – URL: <https://rg.ru/2018/03/14/natalia-kasperskaia-rasskazala-kak-rossii-sohranit-cifrovoj-suverenitet.html> (дата обращения: 28.10.2018).

44. Коваленко, А.П. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) / А.П. Коваленко, Е.Б. Белов. // Научные и методологические проблемы информационной безопасности: сборник статей. – М.: МЦНМО, 2004. С.117-133.
45. Кудрин: серьезные проблемы РФ – слабое техническое развитие и слабые темпы «цифровизации» экономики. – [Электронный ресурс]. – URL: <http://www.interfax.ru/rusinvestforum/551462> (дата обращения: 28.10.2018).
46. Кузьменко, Н.В. Сравнительный анализ стандартизации высшего образования в России и Германии на рубеже XX-XXI веков: дис. ... канд. пед. наук: 13.00.08 / Кузьменко Наталья Васильевна. – Ставрополь, 2009. – 199 с.
47. Куликов, С.Г. Правовые основы обеспечения информационной безопасности РФ и Соединенного Королевства Великобритании и Северная Ирландия / С.Г. Куликов // Актуальные исследования. – 2020. – №19 (22). С. 52-55.
48. Лаборатория Касперского открывает курс стажировки преподавателей вузов [Электронный ресурс]. – URL: [https://www.kaspersky.ru/about/press-releases/2005\\_laboratoriya-kasperskogo-otkryvaet-kurs-stajirovki-prepodavateleii-vuzov](https://www.kaspersky.ru/about/press-releases/2005_laboratoriya-kasperskogo-otkryvaet-kurs-stajirovki-prepodavateleii-vuzov) (дата обращения: 28.10.2018).
49. Лавина, Т.А. ИКТ-компетентность будущих специалистов по защите информации / Т.А. Лавина, Л.А. Ильина // Вестник Череповецкого государственного университета. – 2021. – № 6 (105). – С. 112-128.
50. Лавина, Т.А. Подготовка по информатике будущих специалистов по защите информации: содержательный аспект / Т.А. Лавина, Л.А. Ильина // Вестник Череповецкого государственного университета. – 2020. – № 1 (94). – С. 173-184.
51. Лебедев, А.А. Влияние информационных технологий на конкурентоспособность экономики России / А.А. Лебедев // Российский внешнеэкономический вестник. – 2011. – №9. – С.60-67.
52. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство / В.Н. Лопатин. – М.: Фонд «Университет», 2000. – 428 с.
53. Луговская, И.Р. Параметрический подход к анализу систем школьного

образования разных стран: автореф. дис. ... д-ра. пед. наук: 13.00.01 / Луговская Ирина Робертовна. – Санкт-Петербург, 2004. – 40 с.

54. Лукацкий, А.В. Нужен ли в России CISSP? [Электронный ресурс] / А.В. Лукацкий // – URL: <https://www.itweek.ru/infrastructure/article/detail.php?ID=65988> (дата обращения: 28.10.2018).

55. Лукацкий, А.В. Регулирование безопасности в России усиливается [Электронный ресурс] / А.В. Лукацкий // Директор информационной службы. – 2011. – № 07. – URL: <https://www.osp.ru/cio/2011/07/13009726/> (дата обращения: 28.10.2018).

56. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. / А.А. Малюк. – М: Горячая линия-Телеком, 2004. – 280 с.

57. Манойло, А.В. Современные интерпретации термина «информационная война» / А.В. Манойло // Дневник Алтайской школы политических исследований. – 2012. – № 28. – С. 24-29.

58. Маргаров, Г.И. Воспитание защитников информации / Г.И. Маргаров // Открытые системы. СУБД. – 2009. – № 4. – URL: <https://www.osp.ru/os/2009/04/9298350/> (дата обращения: 28.10.2018).

59. Материалы вебинара «Сложности и спорные вопросы реализации закона «О персональных данных» [Электронный ресурс]. – URL: <https://youtu.be/WKUueUAKfS8> (дата обращения: 28.10.2018).

60. Морозов, А.В. Проблема информационной безопасности личности в условиях цифрового образовательного пространства / А.В. Морозов // Ученые записки ИУО РАО. – 2018. – № 4 (68). – С. 90-94.

61. Морозов, А.В. Проблема национальной безопасности России в условиях цифровизации образовательного пространства / А.В. Морозов // Профессиональное образование в современном мире. – 2019. – Т.9. № 2. – С. 2663-2673.

62. Морозов, А.В. Проблемы безопасности субъектов образовательной среды в процессе их взаимодействия в условиях информационного пространства /

А.В. Морозов // Герценовские чтения: психологические исследования в образовании. – 2018. – № 1-1. – С. 216-223.

63. Морозов, А.В. Проблемы информационной безопасности личности обучающегося в условиях цифровой образовательной среды / А.В. Морозов // Информатизация образования – 2020: международная научно-практическая конференция – Орел: Орловский государственный университет имени И.С. Тургенева, 2020. – С. 286-292.

64. Моцарь, Л.С. О готовности студента вуза к профессиональной деятельности / Л.С. Моцарь, С.Д. Некрасов // Южно-российский журнал социальных наук. – 2011.– № 1. – С. 110-118

65. Никифорова, Г.Г. Формирование безопасной информационной среды для обеспечения творческого потенциала молодого ученого / Г.Г. Никифорова, А.В. Морозов // Казанский вестник молодых ученых. – 2018. – Т.2. № 2 (5). – С. 68-72.

66. О дополнении Классификатора направлений и специальностей высшего профессионального образования [приказ Государственного комитета Российской Федерации по высшему образованию № 911 от 15 июня 1995 года]. – Москва, 1995.

67. О Стратегии национальной безопасности Российской Федерации: [указ Президента Российской Федерации от 02.07.2021 г. № 400]. – Москва, 2021.

68. Об утверждении государственного образовательного стандарта в части Классификатора направлений и специальностей высшего профессионального образования [приказ Государственного комитета Российской Федерации по высшему образованию № 180 от 5 марта 1994 года]. – Москва, 1994.

69. Об утверждении государственных образовательных стандартов высшего профессионального образования [приказ Минобрнауки РФ № 686 от 02 марта 2000 года]. – Москва, 2000.

70. Об утверждении Доктрины информационной безопасности Российской Федерации: [Указ Президента Российской Федерации № 646 от 5 декабря 2016 г.]. – Москва, 2016.

71. Об утверждении Перечня направлений подготовки (специальностей) высшего профессионального образования [приказ Минобрнауки РФ № 4 от 12.01.2005]. – Москва, 2005.
72. Обучение в Лаборатории Касперского. Сертификация [Электронный ресурс]. – URL: <https://support.kaspersky.ru/learning/certification> (дата обращения: 12.02.2020).
73. Околот, Д.Я. Компетентностный подход в подготовке специалистов в области информационной безопасности в учреждениях среднего профессионального образования / Д.Я. Околот, И.Д. Рудинский // Калининградский вестник образования. – 2020. – № 2(6). – С. 35-43.
74. Орехова, Е.Я. Образование во Франции: традиции и реформы: дис. ... д-ра пед. наук: 13.00.01 / Орехова Елена Яковлевна. – Тула, 2004. – 352 с.
75. Плешакова, А.Ю. Генезис педагогической компаративистики в работах западных исследователей / А.Ю. Плешакова // Педагогический журнал Башкортостана. – 2019. – № 4 (83). – С. 68-73.
76. Погорелов, Б.А. О подготовке кадров в области информационная безопасность / Б.А. Погорелов, И.В. Мацкевич // Информационное общество. – 1997. – № 1. – С. 17-22.
77. Положение об учебно-методическом объединении высших учебных заведений Российской Федерации по образованию в области информационной безопасности: [протокол № 1 заседания Совета УМО]. – Москва, 2001.
78. Полушин, Е.О. К вопросу о понятии и сущности информационной войны / Е.О. Полушин // Вестник Московского государственного областного университета. Серия История и политические науки . – 2009. – № 2. – С. 189-193.
79. Поляков, В.П. Аспекты информационной безопасности в информационной подготовке. – М.: ФГБНУ «ИУО РАО», 2016. – 135 с.
80. Поляков, В.П. Педагогические аспекты обеспечения информационной безопасности личности в современной образовательной среде / В.П. Поляков // Национальная безопасность и молодежная политика: киберсоциализация и трансформация ценностей в VUCA-мире. материалы Международной научно-



- практической конференции. – Челябинск: Издательство Южно-Уральского государственного гуманитарно-педагогического университета, 2021. – С. 240-244.
81. Порядок разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности: [Приказ Министерства образования и науки РФ № 1310 от 5 декабря 2013 г]. – Москва, 2013.
82. Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности»: [приказ Минтруда России от 09.11.2016 N 611н]. – Москва, 2016.
83. Пустоцвет, В.С. Сравнительный анализ подготовки педагогических кадров в Германии и России: дис. ... канд. пед.наук: 13.00.08 / Пусвацет Виктория Сергеевна. – Спб., 2007. – 202 с.
84. Российская социологическая энциклопедия / РАН. Ин-т социал.-полит. исслед.; Под общ. ред. акад. РАН Г. В. Осипова. – М.: Норма-Инфра-М, 1998. – 664 с.
85. Рудинский, И.Д. Особенности подготовки специалистов по безопасности компьютерных сетей / И.Д. Рудинский, Д.Я. Околот // Известия Балтийской государственной академии рыбопромыслового флота: психолого-педагогические науки. – 2019. – № 2(48). – С. 141-145.
86. Рудинский, И.Д. Социальные сети образовательного назначения как объект защиты при подготовке специалистов по информационной безопасности / И.Д. Рудинский, Д.Я. Околот // Открытое образование. – 2019. – Т. 23. № 1. – С. 46-56.
87. Савостицкий, Ю.А. История развития глобальных компьютерных сетей / Ю.А. Савостицкий // Информационное общество. – 2000. – № 4. – С. 59 - 65.
88. Самохвалов, А.В. Сотрудничество сетевой академии Cisco и Тамбовского государственного университета в подготовке специалистов-информатиков / А.В. Самохвалов, А.И. Баженов // Психолого-педагогический журнал Гаудеамус. – 2014. – № 2 (24). – С. 214-215.

89. Сетевая Академия Cisco [Электронный ресурс]. – URL: [https://www.cisco.com/c/ru\\_ru/about/net-academy.html](https://www.cisco.com/c/ru_ru/about/net-academy.html) (дата обращения: 28.09.2021).
90. Сетевая академия Cisco. Курсы по информационной безопасности [Электронный ресурс]. – URL: <https://www.netacad.com/courses/security> (дата обращения: 28.09.2021).
91. Слостенин, В. А. Педагогика: учеб. пособие для студентов пед. учеб. заведений 4-е изд. / В.А. Слостенин, И.Ф. Исаев, А.И. Мищенко, Е.Н. Шиянов. – М.: Школьная Пресса, 2004. – 512 с.
92. Солодянников, А.В. Система подготовки специалистов и повышение квалификации в сфере информационной безопасности в зарубежных странах / А.В. Солодянников, А.С. Морозова // Фундаментальные и прикладные исследования в современном мире. –2013. – №4. – С.149-154.
93. Соляной, В.Н. Сертификация бакалавров и магистров информационной безопасности по требованиям профессиональных стандартов с использованием системы дополнительного образования / В.Н. Соляной, А.И. Сухотерин, Т.Ш. Шихнабиева // Актуальные проблемы обеспечения информационной безопасности: труды Межвузовской научно-практической конференции. – Самара: Изд-во Инсома-Пресс, 2017. – С.196-204.
94. Сравнительная педагогика: учебное пособие / Е.В. Андриенко; Мин-во образования и науки РФ, Новосиб. гос. пед. ун-т. – Новосибирск: Изд-во НГПУ, 2016. – 209 с.
95. Стратегия развития отрасли информационных технологий в РФ на 2014-2020 годы и на перспективу до 2025 года [распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р]. – Москва, 2013.
96. Ушаков, Д.Н. Большой толковый словарь современного русского языка / Д.Н. Ушаков. – М.: Альта-Принт [и др.], 2008. – 1239 с.
97. Федеральный государственный стандарт высшего образования по направлению подготовки 10.03.01 «Информационная безопасность»: [приказ Министерства науки и высшего образования РФ №1427 от 17 ноября 2020 года]. – Москва, 2020.

98. Федеральный государственный стандарт высшего образования по направлению подготовки 10.05.01 «Компьютерная безопасность»: [приказ Министерства науки и высшего образования РФ №1459 от 26 ноября 2020 года]. – Москва, 2020.
99. Федеральный государственный стандарт высшего образования по направлению подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем»: [приказ Министерства науки и высшего образования РФ №1458 от 26 ноября 2020 года]. – Москва, 2020.
100. Федеральный государственный стандарт высшего образования по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем»: [приказ Министерства науки и высшего образования РФ №1457 от 26 ноября 2020 года]. – Москва, 2020.
101. Федеральный государственный стандарт высшего образования по направлению подготовки 10.05.04 «Информационно-аналитические системы безопасности»: [приказ Министерства науки и высшего образования РФ №1460 от 26 ноября 2020 года]. – Москва, 2020.
102. Федеральный государственный стандарт высшего образования по направлению подготовки 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»: [приказ Министерства науки и высшего образования РФ №1427 от 17 ноября 2020 года]. – Москва, 2020.
103. Федеральный государственный стандарт высшего образования по направлению подготовки 10.04.01 «Информационная безопасность»: [приказ Министерство науки и высшего образования РФ №1461 от 26 ноября 2020 года]. – Москва, 2020.
104. Федорова, М.Ю. Нормативно-правовое обеспечение образования: учеб. пособие для студ. высш. пед. учеб. заведений / М.Ю. Федорова. – 2-е изд., стер. – М.: Издательский центр «Академия», 2009. – 192 с.
105. Фетискин, Н.П. Социально-психологическая диагностика развития личности и малых групп: учеб. пособие для студентов вузов / Н.П. Фетискин, В.В. Козлов, Г.М. Мануйлов. – М.: Изд-во Ин-та Психотерапии, 2002. – 488 с.

106. Филиппова, К.А. Формирование самооценки у студентов гуманитарного вуза в учебно-профессиональной деятельности: дис. ... канд. пед. наук: 13.00.08 / Филиппова Кристина Александровна. – М., 2012. – 168 с.
107. Фишман, Л.И. Логика управления школой: пособие по курсу «Теория управления педагогическими системами». Серия: Подготовка менеджеров образования / Л.И. Фишман. – Самара: СИПКРО, 1996. – 116 с.
108. ФСТЭК РФ. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00> (дата обращения: 28.10.2018).
109. Храмова, М.В. Формирование готовности специалистов к профессиональной деятельности на основе использования технологий дистанционного обучения: дис. ... канд. пед. наук: 13.00.08 / Храмова Марина Викторовна. – М., 2000. – 233 с.
110. Чванова, М.С. Кластерный подход к подготовке специалистов по информационной безопасности / М.С. Чванова, Е.М. Михайлова, Д.В. Лопатин, В.Ю. Лыскова, М.С. Анурьева // Психолого-педагогический журнал Гаудеамус. – 2013. – № 2. – С. 48-53.
111. Чванова, М.С. Методологические и теоретические основы информатизации системы непрерывной подготовки специалистов Т.1: дис. ... д.-ра пед. наук: 13.00.08 / Чванова Марина Сергеевна. – М., 1999. – 365 с.
112. Чванова, М.С. Отечественный и зарубежный опыт включения вендорских образовательных курсов в подготовку специалистов по информационной безопасности / М.С. Чванова, М.С. Анурьева // Человеческий капитал. – 2021. – № 12 (156). – С. 145-149.
113. Чванова, М.С. Подготовка кадров в области информационной безопасности в США / М.С. Чванова, М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – Т. 112. № 8. – С. 126-133.

114. Чванова, М.С. Подготовка специалистов в области информационной безопасности: инновационный подход к формированию образовательной среды / М.С. Чванова, М.С. Анурьева, В.Ю. Лыскова, Н.А. Котова, А.А. Молчанов // Психолого-педагогический журнал Гаудеамус. – 2015. – № 1 (25). – С. 18–31.
115. Чванова, М.С. Подготовка специалистов в области информационной безопасности во Франции / М.С. Чванова, М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – Т. 111. № 7. – С. 159–165.
116. Чванова, М.С. Система высшего образования в ФРГ. Подготовка специалистов в области информационной безопасности/ М.С. Чванова, М.С. Анурьева // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2012. – Т. 110. № 6. – С. 78–84.
117. Шерстюк, В.П. О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности/ В.П. Шерстюк // Научные и методологические проблемы ИБ (сборник статей) – М.: МЦНМО, 2004. –С.37-45.
118. Широбоков, С.Н. Концептуализация сравнительной педагогики / С.Н. Широбоков // Наука о человеке: гуманитарные исследования. – 2019. – № 4(38). – С. 66-69.
119. Шкуратова, А.П. Методология системного подхода в педагогике / А.П. Шкуратова // Труды БрГУ. Серия: Естественные и инженерные науки. – 2014. – Т. 1. – С.255-259.
120. Яковлева, Н.О. Информационный подход в педагогических исследованиях: сущность, значение, особенности реализации / Н.О. Яковлева // Вестник ЮУрГУ. Серия: Образование. Педагогические науки. – 2009. – № 1 (134). – С.16-22.
121. Янкевич, К.А. Разграничении понятий «образовательная система» и «система образования» / К.А. Янкевич // Вестник северо-восточного государственного университета. – 2007. – № 8 – С.130-132.
122. A brief history of internet security [Электронный ресурс]. – URL: <https://www.scmagazine.com/a-brief-history-of-internet-security/article/556389/> (дата обращения: 28.10.2018).
123. Ariyapperuma, S. Web-based curriculum as a pedagogic tool for e-learning, in

network security / S. Ariyapperuma, K. Minhas // 34th Annual Frontiers in Education. – 2004. – CC. T2C-1- T2C-1.

124. Association de Cryptographie Théorique et Appliquée [Электронный ресурс]. – URL: <http://www.acrypta.com/> (дата обращения: 25.08.2018).

125. Bremen Universität [Электронный ресурс]. – URL: <https://www.uni-bremen.de/master/master-of-science.html> (дата обращения: 25.08.2018).

126. Brown, R. A Survey on CISSP (Certified Information Systems Security Professional) Contributions to Higher Education Research / R. Brown // Proceedings of the EDSIG Conference. – 2019. – V.5 № 4954. – С.1-5.

127. Brown, R. The Contribution of the CISSP to Higher Education Research / R. Brown // Information Systems Education Journal. – 2019. – V.17 № 3. – С.50-54.

128. Campus Gelsenkirchen [Электронный ресурс]. – URL: <https://www.w-hs.de/flyer-master-ge/> (дата обращения: 25.08.2018).

129. Champlain College, Network Security & Administration Degree (BS) [Электронный ресурс]: сайт. – URL: <http://online.champlain.edu/network-security-administration/bachelors-degree> (дата обращения: 25.08.2018).

130. Computer and Information Security BSc (Honours) [Электронный ресурс]. – URL: <http://www.shu.ac.uk/prospectus/course/630/> (дата обращения: 25.08.2018).

131. Computer Forensics and Security BSc (Hons) [Электронный ресурс]. – URL: <https://www2.mmu.ac.uk/course/bsc-computer-forensics-and-security/> (дата обращения: 25.08.2018).

132. Computer Forensics BSc (Hons) [Электронный ресурс]. – URL: <http://courses.glam.ac.uk/courses/563-bsc-hons-computer-forensics> (дата обращения: 25.08.2018).

133. Computer Forensics, London Met [Электронный ресурс]. – URL: <http://www.londonmet.ac.uk/courses/undergraduate/digital-forensics-and-cyber-security---bsc-hons/> (дата обращения: 25.08.2018).

134. Computer Forensics, University of Westminster [Электронный ресурс]. – URL: <http://courses.westminster.ac.uk/CourseSearch.aspx> (дата обращения: 25.08.2018).

135. Computer Network Security [Электронный ресурс]. – URL: <https://www.westminster.ac.uk/computer-and-network-engineering-courses/2018-19/september/full-time/computer-network-security-bsc-honours> (дата обращения: 25.08.2018).
136. Computer Networks and Security [Электронный ресурс]. – URL: <http://www.staffs.ac.uk/course/computer-networks-security-bsc-msci> (дата обращения: 25.08.2018).
137. Computer Networks and Security Masters [Электронный ресурс]. – URL: [http://www.mdx.ac.uk/courses/postgraduate/computing\\_and\\_it/comp\\_net\\_security\\_msc.aspx](http://www.mdx.ac.uk/courses/postgraduate/computing_and_it/comp_net_security_msc.aspx) (дата обращения: 25.08.2018).
138. Computer Sciences – основные вехи [Электронный ресурс] // Открытые системы. – 1997. – № 5. – URL: <https://www.osp.ru/os/1997/05/179286/> (дата обращения: 12.11.2018).
139. Computer Security and Resilience MSc [Электронный ресурс]. – URL: <https://www.ncl.ac.uk/postgraduate/courses/degrees/computer-security-resilience-msc/#profile> (дата обращения: 25.08.2018).
140. Computer Security BEng(Hons), BSc(Hons) [Электронный ресурс]. – URL: <http://www.staffs.ac.uk/course/cyber-security-bsc> (дата обращения: 25.08.2018).
141. Computer Security BSc (Hons) [Электронный ресурс]. – URL: <http://www.dmu.ac.uk/study/courses/undergraduate-courses/computer-security-bsc-degree/computer-security-bsc-hons-degree.aspx> (дата обращения: 25.08.2018).
142. Computer Security with Forensics BSc (Honours) [Электронный ресурс]. – URL: <https://www.shu.ac.uk/courses/computing/bsc-honours-computer-security-with-forensics/full-time/2018/> (дата обращения: 25.08.2018).
143. Computing and Law [Электронный ресурс]. – URL: [http://www.herts.ac.uk/gsa\\_courses/Computing-and-Law.cfm](http://www.herts.ac.uk/gsa_courses/Computing-and-Law.cfm) (дата обращения: 25.08.2018).
144. Coursesat London Met [Электронный ресурс]. – URL: <http://www.londonmet.ac.uk/courses/> (дата обращения: 25.08.2018).

145. Craig Timberg A history of Internet security [Электронный ресурс]. – URL: <https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/> (дата обращения: 25.08.2018).
146. Cryptographieet Sécurité Informatique [Электронный ресурс]. – URL: <http://www.master-secrets.uvsq.fr/index.php> (дата обращения: 25.08.2018).
147. Cryptologieet sécurité informatique [Электронный ресурс]. – URL: <http://www.u-bordeaux1.fr/ufr/math-info/formation/mathematiques-pures/master/csi-cryptologie-et-securite-informatique.html> (дата обращения: 25.08.2018).
148. Cyber Security MSc course from De Montfort University [Электронный ресурс]. – URL: <http://www.dmu.ac.uk/study/courses/postgraduate-courses/cyber-security/cyber-security-msc-degree.aspx> (дата обращения: 25.08.2018).
149. Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberspace [Электронный ресурс]. – URL: <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la> (дата обращения: 28.03.2021).
150. Die Hochschule Offenburg [Электронный ресурс]. – URL: <http://www.fh-offenburg.de/uportal/go.jsp?id=1&l=de> (дата обращения: 25.08.2018).
151. Exemplarischer Studienverlauf: Unternehmens- und IT-Sicherheit (B.Sc.) [Электронный ресурс]. – URL: [https://mi.hs-offenburg.de/fileadmin/Einrichtungen/Fakultaet\\_M\\_I/Fakultaetsseite/files/unternehmen-s-it-sicherheit-bachelor-studienverlauf.pdf](https://mi.hs-offenburg.de/fileadmin/Einrichtungen/Fakultaet_M_I/Fakultaetsseite/files/unternehmen-s-it-sicherheit-bachelor-studienverlauf.pdf) (дата обращения: 25.08.2018).
152. Forensic Computing. [Электронный ресурс]. – URL: [http://www.staffs.ac.uk/courses\\_and\\_study/courses/forensic-computing-tcm4212233.jsp](http://www.staffs.ac.uk/courses_and_study/courses/forensic-computing-tcm4212233.jsp) (дата обращения: 25.08.2018).
153. Forensic Computing MSc [Электронный ресурс]. – URL: <http://www.dmu.ac.uk/study/courses/forensic-computing-for-practitioners-professional-qualification.aspx> (дата обращения: 25.08.2018).



154. Gapinski, A.J. Certificate Programs in Computer Networks, Security, and Cloud Computing in the USA – A Review / A.J. Gapinski // Journal: E-mentor. – 2017. – №4. – С.64-78.
155. George Washington University, Networking professionals and communications specialists [Электронный ресурс]. – URL: <http://nearyou.gwu.edu/tc/index1.html> (дата обращения: 25.08.2018).
156. Grover, M. How secure is education in Information Technology? / M. Grover, B. Reinicke // Information Systems Education Journal. 2016. – V.14 №3. – С.29-44
157. Hochschule Aalen [Электронный ресурс]. – URL: <http://www.htw-aalen.de/> (дата обращения: 25.08.2018).
158. Informatik (Bachelor of Science, Ein-Fach) [Электронный ресурс]. – URL: <https://www.uni-bonn.de/studium/vor-dem-studium/faecher/informatik/informatik-bachelor-of-science/informatik-bachelor-of-science-ein-fach> (дата обращения: 25.08.2018).
159. Informatik. Informationen der Zentralen Studienberatung [http](http://www3.uni-bonn.de/studium/studienangebot/grundstaendige-studiengaenge/informatik) [Электронный ресурс]. – URL: <http://www3.uni-bonn.de/studium/studienangebot/grundstaendige-studiengaenge/informatik> (дата обращения: 25.08.2018).
160. Information Security Systems [Электронный ресурс]. – URL: <http://www.uel.ac.uk/programmes/cite/undergraduate/security.html> (дата обращения: 25.08.2018).
161. Information Systems Security MSc [Электронный ресурс]. – URL: <https://www.shu.ac.uk/courses/computing/msc-information-systems-security/full-time/2018> (дата обращения: 25.08.2018).
162. Information Technology Security MSc [Электронный ресурс]. – URL: <http://courses.westminster.ac.uk/CourseSearch.aspx> (дата обращения: 25.08.2018).
163. Informations technologierecht und Recht des geistigen Eigentums (Bachelor of Laws) [Электронный ресурс]. – URL: <https://www.uni-hannover.de/de/studium/informationstechnologierecht-und-recht-des-geistigen-eigentums/> (дата обращения: 25.08.2018).
164. Informations technologierecht und Recht des geistigen Eigentums (Master of Laws) [Электронный ресурс]. – URL: <https://www.uni->

- hannover.de/de/studium/informationstechnologierecht-und-recht-des-geistigen-eigentums-1/  
(дата обращения: 25.08.2018).
165. IT Security [Электронный ресурс]. – URL: <http://www.londonmet.ac.uk/ug-prospectus/courses-11-12/it-security.cfm> (дата обращения: 25.08.2018).
166. IT Security MSc [Электронный ресурс]. – URL: <http://www.londonmet.ac.uk/pgprospectus/courses/it-security.cfm> (дата обращения: 25.08.2018).
167. IT-Sicherheit Bachelor of Science [Электронный ресурс]. – URL: <https://www.hs-aalen.de/de/courses/23> (дата обращения: 25.08.2018).
168. John von Neumann. First Draft of a Report on the EDVAC. University of Pennsylvania [Электронный ресурс]. – URL: <https://web.mit.edu/STS.035/www/PDFs/edvac.pdf>
169. Karlsruhe UKIT [Электронный ресурс]. – URL: <http://www.kit.edu/studieren/2459.php> (дата обращения: 25.08.2018).
170. Leibniz Universität Hannover [Электронный ресурс]. – URL: <http://www.uni-hannover.de/de/studium/studienfuehrer/it-recht/index.php> (дата обращения: 25.08.2018).
171. Lotter, M. Einbettung industrieller IT-Qualifizierungsangebote in die berufliche Erstausbildung / Lotter M. // Lernen & lehren. 2015. – №2. – С.70-75.
172. Madison Area Technical College, IT-Network Security Specialist [Электронный ресурс]. – URL: <http://programs.matcmadison.edu/programs/it-network-security-specialist/> (дата обращения: 25.08.2018).
173. Marquardson, J. Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs / J. Marquardson; A. Elnoshokaty // Information Systems Education Journal. 2020. – v18 №1. – С. 22-28
174. Master Informatik. Kurzbeschreibung [Электронный ресурс]. – URL: <http://www.uni-passau.de/master-informatik/> (дата обращения: 25.08.2018).
175. Mastère spécialisé Technologies du Web et Cyber-sécurité [Электронный ресурс]. – URL: <https://www.imt-atlantique.fr/fr/formation/masteres-specialises> (дата обращения: 25.08.2018).

176. Mathématiques de l'information, Cryptographie [Электронный ресурс]. – URL: <http://etudes.univ-rennes1.fr/master-crypto/themes/Objectifs> (дата обращения: 25.08.2018).
177. Mercy College, Master of Science Cybersecurity [Электронный ресурс]. – URL: <https://www.mercy.edu/academics/programs/cybersecurity-0> (дата обращения: 25.08.2018).
178. Mike Lynett A History of Information Security From Past to Present [Электронный ресурс]. – URL: <http://blog.mesltd.ca/a-history-of-information-security-from-past-to-present> (дата обращения: 25.08.2018).
179. Mount Aloysius College, Degree Detail [Электронный ресурс]. – URL: [http://www.mtaloy.edu/academics/degree\\_detail.dot?inode=465881](http://www.mtaloy.edu/academics/degree_detail.dot?inode=465881) (дата обращения: 25.08.2018).
180. MSc Computer Security [Электронный ресурс]. – URL: <http://www.essex.ac.uk/coursefinder/CourseDetails.aspx?course=MSC+G49324> (дата обращения: 25.08.2018).
181. Murphy, G. Abstraction In Computer Network Education: A Model Based Approach / G. Murphy, G. Kohli, S.P. Maj, D. Veal // Paper presented Annual Conference, Salt Lake City, Utah. – 2004. – С.9.134.1-9.134.8
182. Network Management and Security [Электронный ресурс]. – URL: [http://www.mdx.ac.uk/courses/network\\_management\\_and\\_security\\_bsc.aspx](http://www.mdx.ac.uk/courses/network_management_and_security_bsc.aspx) (дата обращения: 25.08.2018).
183. Network Management and Security MSc [Электронный ресурс]. – URL: <http://www.londonmet.ac.uk/courses/postgraduate/computer-networking-and-cyber-security-with-work-experience---msc/> (дата обращения: 25.08.2018).
184. Network Security MSc [Электронный ресурс]. – URL: <https://www.anglia.ac.uk/science-and-technology/cyber-security-and-networking-research-group> (дата обращения: 25.08.2018).
185. Organisation et Protection des Systèmes d'Information dans les Entreprises. [Электронный ресурс]. – URL: <http://www.univ-lyon2.fr/master-2-organisation-et-protection-des-systemes-d-information-dans-les-> (дата обращения: 25.08.2018).

186. Profil des Studiengangs InternetSicherheit [Электронный ресурс]. – URL: [https://www.w-hs.de/Master/Internet\\_Sicherheit\\_GE\\_Master.pdf](https://www.w-hs.de/Master/Internet_Sicherheit_GE_Master.pdf) (дата обращения: 25.08.2018).
187. Sécurité Informatique. [Электронный ресурс]. – URL: <https://www.unilim.fr/master/masters-securite-informatique/> (дата обращения: 25.08.2018).
188. Smith, A. Large scale delivery of Cisco Networking Academy Program by blended distance learning / A. Smith, N. Moss // In: IARIA 2010 Sixth International Conference on Networking and Service. – 2010. – С.329-334.
189. South Mountain Community College, Information Technology IT: Network Security. [Электронный ресурс] – URL: <http://infotech.southmountaincc.edu/Programs/NetworkSecurity/Degree.htm> (дата обращения: 25.08.2018).
190. Southern Oregon University, Computer Security and Information Assurance Option, BA or BS. [Электронный ресурс]. – URL: [http://catalog.sou.edu/preview\\_program.php?catoid=2&pooid=262](http://catalog.sou.edu/preview_program.php?catoid=2&pooid=262) (дата обращения: 25.08.2018).
191. St Cloud State University Computer Networking and Applications (CNA) Undergraduate Programs. [Электронный ресурс]. – URL: <http://bulletin.stcloudstate.edu/ugb/programs/cna.asp> (дата обращения: 25.08.2018).
192. St Johns University, Computer Security Systems [Электронный ресурс] – URL: <http://www.stjohns.edu/academics/csms/degree/csecs> (дата обращения: 25.08.2018).
193. Strayer University, Bachelor of Science in Criminal Justice [Электронный ресурс]. – URL: <http://www.strayer.edu/program/bachelor-science-criminal-justice> (дата обращения: 25.08.2018).
194. Technische Hochschule Brandenburg University of Applied Science [Электронный ресурс]. – URL: <http://fbwcms.fh-brandenburg.de/de/5185> (дата обращения: 25.08.2018).
195. Ted Julian Defining Moments in the History of Cyber-Security and the Rise of Incident Response [Электронный ресурс]. – URL: <https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/> (дата обращения: 12.11.2018).

196. Texas State Technical College – Waco, Network Security Technologies (NST) [Электронный ресурс]. – URL: <http://cns.tstc.edu/tdean/> (дата обращения: 25.08.2018).
197. The University of Tennessee Chattanooga, Valid Programs and Minors [Электронный ресурс]. – URL: <https://new.utc.edu/enrollment-management-and-student-affairs/registrar/current-programs#cecs> (дата обращения: 25.08.2018).
198. Tompkins-Cortland Community College, Computer Forensics [Электронный ресурс]. – URL: [http://www.tc3.edu/catalog/ap\\_program.asp?dp=computer\\_forensics](http://www.tc3.edu/catalog/ap_program.asp?dp=computer_forensics) (дата обращения: 25.08.2018).
199. Univ. Grenoble Alpes [Электронный ресурс]. – URL: <https://www.univ-grenoble-alpes.fr/> (дата обращения: 25.08.2018).
200. Universität Passau [Электронный ресурс]. – URL: <http://www.uni-passau.de/> (дата обращения: 25.08.2018).
201. Université de Caen Basse Normandie E-SECURE [Электронный ресурс]. – URL: <https://uniform.unicaen.fr/catalogue/formation/master/5705-master-informatique-parcours-securite-des-systemes-informatiques?s=&r=> (дата обращения: 25.08.2018).
202. Université de Caen Basse-Normandie Licence Pro Audit et sécurité des réseaux et des systèmes d'information [Электронный ресурс]. – URL: [http://www.unicaen.fr/LPSECUR\\_911/0/ficheformation/&RH=1279179135480](http://www.unicaen.fr/LPSECUR_911/0/ficheformation/&RH=1279179135480) (дата обращения: 25.08.2018).
203. University of Tennessee At Chattanooga [Электронный ресурс]. – URL: [http://www.utc.edu/Research/Cisa/concentration.php#\\_B.S.\\_Computer\\_Science](http://www.utc.edu/Research/Cisa/concentration.php#_B.S._Computer_Science) (дата обращения: 25.08.2018).
204. Unternehmens und IT [Электронный ресурс]. – URL: <https://mi.hs-offenburg.de/studium/bachelor-studiengaenge/unternehmen-und-it-sicherheit/> (дата обращения: 25.08.2018).
- .

## СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Номер и наименование рисунка (таблицы)	Страница
Рисунок 1 – Отечественная система образования в области ИБ и ее взаимосвязь со сферой профессиональной деятельности	29
Рисунок 2 – Количество реализовавшихся образовательных программ по уровням подготовки в 2010 и 2011 годах	30
Рисунок 3 – Количество реализовавшихся образовательных программ по уровням подготовки в 2016 году	31
Рисунок 4 – Интеграция профессиональных стандартов по информационной безопасности и образовательных стандартов	32
Рисунок 5 – Количество программ бакалавриата, специалитета и магистратуры по направлениям подготовки и специальностям (2016 год)	35
Рисунок 6 – Схема уровней подготовки будущих специалистов в области информационной безопасности и укрупненных блоков в Великобритании	41
Рисунок 7 – Укрупненные блоки образовательных программ по информационной безопасности в Великобритании	43
Рисунок 8 – Соотношение числа образовательных программ бакалавриата по укрупненным блокам в Великобритании, %	44
Рисунок 9 – Соотношение количества программ поствысшего образования по укрупненным блокам в Великобритании, %.	48
Рисунок 10 – Соотношение количества магистерских программ по укрупненным блокам в Великобритании, %.	48
Рисунок 11 – Укрупненные блоки образовательных программ по информационной безопасности в США	52
Рисунок 12 – Схема уровней подготовки по ИБ и укрупненные блоки образовательных программ в США	53
Рисунок 13 – Соотношение количества образовательных программ бакалавриата по направлениям подготовки в США, %	54
Рисунок 14 – Соотношение количества образовательных программ магистратуры по направлениям подготовки в США, %	55
Рисунок 15 – Общая схема ступеней профессионального образования специалистов по информационной безопасности в Германии	58
Рисунок 16 – Схема присуждаемых во Франции дипломов о высшем образовании	65
Рисунок 17 – Критерии сопоставления педагогических систем профессионального образования будущих специалистов по информационной безопасности	98
Таблица 1 – Сопоставление систем профессионального образования будущих специалистов по информационной безопасности в России и за рубежом	101-105
Рисунок 18 – Общие черты и ключевые различия систем профессионального образования в России, США, Великобритании, Германии, Франции	113
Таблица 2 – Результаты сравнительно-сопоставительного анализа в соответствии с методологическими подходами	119-120
Рисунок 19 – Компоненты модернизации содержательной составляющей отечественной системы образования специалистов и механизмы их реализации	121
Таблица 3 – Критерии и диагностический инструментарий уровня готовности студентов к будущей профессиональной деятельности	132
Таблица 4 – Характеристика компонентов готовности студентов к будущей профессиональной деятельности на низком, среднем и высоком уровнях ее сформированности	133-134
Рисунок 20 – Распределение мотивов по шкалам в КГ и ЭГ на констатирующем этапе эксперимента, %	137
Таблица 5 – Результат самооценки студентов умений и навыков на констатирующем этапе эксперимента	139

Таблица 6 – Результаты оценки уровней готовности студентов к будущей профессиональной деятельности по критериям на констатирующем этапе	142-143
Рисунок 21 – Результаты оценки уровня готовности студентов к будущей профессиональной деятельности по критериям на констатирующем этапе, %	143
Таблица 7 – Распределение мотивов по шкалам в КГ и ЭГ до и после проведения опытно-экспериментальной работы	145
Рисунок 22 – Уровень развития мотивационного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.	146
Рисунок 23 – Уровень развития когнитивного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %.	147
Таблица 8 – Результат самооценки студентов умений и навыков в КГ и ЭГ до и после опытно-экспериментальной работы	148
Рисунок 24 – Уровень развития деятельностного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %	149
Рисунок 25 – Уровень развития эмоционально-оценочного критерия до и после опытно-экспериментальной работы в КГ и ЭГ, %	151
Таблица 9 – Динамика уровня развития по мотивационному, когнитивному, деятельностному и эмоционально-оценочному критериям студентов в КГ и ЭГ	152
Таблица 10 – Итоговый уровень готовности студентов к будущей профессиональной деятельности в ЭГ и КГ после проведения опытно-экспериментальной работы	152
Рисунок 26 – Итоговое сравнение результатов общего уровня готовности студентов к будущей профессиональной деятельности, %.	153
Таблица 11 – Результаты статистической обработки данных до и после проведения опытно-экспериментальной работы	155-156

## ПРИЛОЖЕНИЕ А

## Содержание образовательных программ в блоке безопасность информационных технологий, бакалавриат (Великобритания)

Таблица Б.1 – Содержание образовательных программ в блоке безопасность информационных технологий, бакалавриат (Великобритания)

	<b>Безопасность информационных систем (Information Security Systems BSc)</b> <b>Университет Восточного Лондона</b>	<b>Безопасность информационных технологий (Information Technology Security BSc)</b> <b>Лондонский Университет Метрополитен</b>	<b>Компьютерная и информационная безопасность (Computer and Information Security BSc)</b> <b>Университет Хэффлэлла Халлама</b>
1 г о д	-«Введение в компьютерные системы» (Introduction to Computer Systems); -«Введение в разработку ПО» (Introduction to Software Development); и др.	-«Архитектура компьютерного оборудования и программного обеспечения» (Computer Hardware and Software Architecture); -«Введение в Интернет» (Introduction to the Internet); -«Введение в криминологию» (Introduction to Criminology); -«Введение в программирование» (Introduction to Programming); -«Логика» (Logic); -«Проблемные задачи для ИТ» (Problem Solving for IT); -«Программирование» (Further Programming)	-«Введение в компьютерную безопасность» (Introduction to computer security); -«Компьютерные технологии» (Computer technology); -«Введение в сети» (Introduction to networks); -«Основы программирования» (Fundamentals of programming); -«Математика» (Mathematics); -«Профессиональные и коммуникабельные навыки» (Professional and communication skills)
2 г о д	-«Технологии и сетевых систем» (Network Systems and Technologies); -«Профессиональные задачи в ИКТ» (Professional Issues in ICT); -«Системы баз данных» (Data base systems);	-«Использование вычислений в компьютерах» (Employment Skillsfor Computing); -«Моделирование данных и системы баз данных» (Data Modelling and Database Systems);	-«Метод проектов» (Project-based learning); -«Беспроводные сети» (Wireless lans ); -«Сетевые технологии» (Network technologies); -«Интерактивная мультимедиа» (Interactive multimedia)
3 г о д	-«Безопасность сетей» (Network Security); -«Цифровые расследования» (Digital Forensics); -«Аудит ИБ» (Information Security Audit and Assurance);  -Дипломный проект	-«Приложения для электронной коммерции» (eCommerce Applications); -«Принципы безопасности сетей» (Principles of Network Security); -«Базовый курсу правления безопасности» (Fundamentals of Security Management);  -Дипломный проект (Final Year Project)	-«Безопасность веб- приложений» (Websecurity ); -«Сети» (Advanced networking); -«Мультимедиа сети» (Multimedia networks ); -«Разработка и мониторинг сетей» (Network design and monitoring); -«Распределенные вычисления» (Distributed computing); -«Технологии мобильных компьютеров» (Mobile computing technologies); -Дипломный проект



## ПРИЛОЖЕНИЕ Б

**Учебный план образовательной программы «Информационная безопасность»  
университета Чаттануга**

Таблица В.1 – Учебный план образовательной программы «Информационная безопасность» университета Чаттануга. Специализированные дисциплины по направлению.

Дисциплина (модуль)	Описание
<b>Принципы информационной безопасности</b>	<p><b>Цели и задачи дисциплины:</b> курс специализируется на информационной безопасности, целостности и конфиденциальности данных. Рассматриваются природа и проблемы компьютерной безопасности, политики безопасности, роль и применение криптографии, методология и технологии анализа уязвимостей и обнаружения вторжений.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- введение в информационную безопасность;</li> <li>- потребность в безопасности;</li> <li>- юридические, этические и профессиональные вопросы в сфере информационной безопасности;</li> <li>- управление рисками;</li> <li>- планирование мер безопасности;</li> <li>- технологии безопасности: межсетевые экраны и виртуальные частные сети;</li> <li>- технологии безопасности: обнаружение вторжений, контроль доступа, средства безопасности;</li> <li>- криптография;</li> <li>- физическая безопасность;</li> <li>- реализация информационной безопасности;</li> <li>- безопасность персонала;</li> <li>- техническое обслуживание систем безопасности</li> </ul>
<b>Безопасность компьютерных сетей</b>	<p><b>Цели и задачи дисциплины:</b> курс посвящен вопросам безопасности компьютерных и мобильных сетей связи. Рассматриваются оценки рисков, политики безопасности, обнаружения вторжений в сеть, экспертиза, современные тенденции и исследования в области безопасности компьютерных сетей.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- враждебные сценарии;</li> <li>- оценка и анализ безопасности;</li> <li>- контроль доступа и авторизация;</li> <li>- проверка подлинности;</li> <li>- криптография;</li> <li>- брандмауэры;</li> <li>- системы обнаружения и предотвращения вторжений;</li> <li>- компьютерные и сетевые экспертизы;</li> <li>- антивирусная и контентная фильтрация;</li> <li>- безопасность Оценка безопасности компьютерных продуктов;</li> <li>- безопасность компьютерных сетей. Протоколы и стандарты;</li> <li>- безопасность беспроводных сетей и устройств;</li> <li>- взгляд в будущее.</li> </ul>
<b>Биометрия и криптография</b>	<p><b>Цели и задачи дисциплины:</b> курс охватывает основные понятия распознавания образов, основы биометрических технологий, а также критическое исследование криптографических протоколов, используемых в приложениях безопасности.</p> <p><b>Содержание:</b> лекции:</p> <ul style="list-style-type: none"> <li>- введение в биометрию;</li> <li>- биометрия отпечатков пальцев;</li> </ul>

Дисциплина (модуль)	Описание
	<ul style="list-style-type: none"> <li>-биометрия лица, анализ главных компонент, линейный анализ, дискриминантный анализ;</li> <li>-графология, образцы почерка, руководящие принципы для графологической экспертизы, NIST-формы на основе системы отпечатков руки;</li> <li>-голосовая биометрия;</li> <li>-ДНК биометрия;</li> <li>-будущее биометрии, проблемы, оценка перспектив;</li> <li>-классическая криптография;</li> <li>-центр распространения ключей;</li> <li>-шифрование на основе открытых ключей;</li> <li>-управление ключами;</li> <li>-проверка подлинности;</li> <li>-Hash ключи;</li> <li>-аутентификация;</li> <li>-квантовая криптография</li> </ul> <p>практические проекты:</p> <ul style="list-style-type: none"> <li>-классификация отпечатков пальцев (PCASYSX, MINDTCT, NFIQ, BOZORTH3);</li> <li>-биометрическое программное обеспечение;</li> <li>-тестирование и документирование распознавания на основе СПС, LDA и байесовских сетей;</li> <li>-распознавание рукописного текста;</li> <li>-распознавание голоса;</li> <li>-асимметричные ключи для шифрования Key Pair Generator;</li> <li>-симметричное шифрование и дешифрование;</li> <li>-единый вход в систему с использованием протокола Kerberos;</li> <li>-функции безопасности в Java SE;</li> <li>-определение корневых центров сертификации</li> </ul>
<b>Управление информационной безопасностью</b>	<p><b>Цели и задачи дисциплины:</b> курс включает вопросы обеспечения безопасности, политики информационной безопасности, разработку программ обеспечения безопасности, контроля доступа, шифрование, управление рисками, реагирование на инциденты</p> <p><b>Содержание:</b> лекции:</p> <ul style="list-style-type: none"> <li>-управление рисками: выявление, оценка и управление;</li> <li>-механизмы защиты, протоколы IPSec и Web Security;</li> <li>-персонал и безопасность;</li> <li>-правовые и этические проблемы;</li> <li>-управления проектами</li> </ul> <p>лабораторные работы:</p> <ul style="list-style-type: none"> <li>-симметричное и асимметричное шифрование;</li> <li>-безопасность электронной почты;</li> <li>-брандмауэры;</li> <li>-контроль доступа: DAC, MAC и RBAC</li> </ul>
<b>Анализ уязвимостей и аудит</b>	<p><b>Цели и задачи дисциплины:</b> курс посвящен оценке уязвимости системных ресурсов, системам обнаружения вторжений и предотвращения несанкционированного доступа.</p> <p><b>Содержание:</b> лекции:</p> <ul style="list-style-type: none"> <li>-обзор компьютерной безопасности, потребность в безопасности</li> <li>-матрица контроля доступа;</li> <li>-политика безопасности;</li> <li>-политика Конфиденциальности;</li> <li>-целостность политики;</li> <li>-гибридные политики;</li> <li>-основы криптографии;</li> <li>-аутентификация;</li> <li>-анализ уязвимостей;</li> <li>-обнаружение вторжений;</li> <li>-сетевая безопасность, введение в сети, сетевые протоколы</li> </ul>

Дисциплина (модуль)	Описание
	лабораторные работы: -анализ рисков; -сканер уязвимостей NMAP; -системы обнаружения вторжений; -сети на основе VPN; -брандмауэры
<b>Безопасность баз данных и аудит</b>	<p><b>Цели и задачи дисциплины:</b>            курс предоставляет обзор систем безопасности баз данных, модели безопасности, аудит баз данных, XML, контроль доступа, доверительное управление.</p> <p><b>Содержание:</b>            лекции:            -основы баз данных, SQL;            -основы операционной системы безопасности;            -администрирование, профили, политика паролей, привилегий и ролей;            -база данных. Модель безопасности приложений;            -многоуровневая безопасность реляционной модели;            -модели управления доступом: MAC , DAC, RBAC;            -хранимые процедуры и функции: PL / SQL , PL / SQL-II;            -виртуальные частные базы данных , SQL-инъекции;            -ревизионные базы данных;            -XML. Контроль доступа;            -водяные знаки в реляционных базах данных;            -защита конфиденциальности;            -доверительное управление;            -управление цифровыми правами</p> <p>проекты:            -установка базы данных;            -реализация дискретного управление доступом;            -реализация обязательного контроля доступа с использованием Oracle Label Security            -хранимые процедуры PL / SQL;            -виртуальные частные базы данных;            -SQL инъекции</p> <p><b>Формы работы:</b>            . Работа над проектом</p>

## ПРИЛОЖЕНИЕ В

### Укрупненные блоки направлений подготовки магистров по информационной безопасности в США

Таблица Г.1 – Укрупненные блоки направлений подготовки магистров по информационной безопасности в США и соответствующие им образовательные программы.

Блок	Образовательные программы
1. Информационная безопасность	-Магистр информационных технологий – Информационная безопасность (M.S. in Information Technology - Information Security); -Магистр технологии и управления–Информационная безопасность (M.S. in Technology Management - Information Security); -Магистр информационной безопасности (M.S. in Information Security); -Магистр технологий – Информационная безопасность (M.S. in Technology - Information Security)
2. Компьютерная безопасность	-Магистр систем безопасность и защиты–Системы (M.S. in System Safety and Security – Systems); -Магистр компьютерных систем; – Управление компьютерной безопасностью(M.S. in Information Systems - Computer Security Management)
3. Расследование компьютерных инцидентов	-Магистр компьютерных и информационных технологий – Виртуальные преступления (M.S.in Computer and Information Technology – Cybe rForensics)
4. Безопасность компьютерных сетей	-Магистр компьютерных наук – Компьютерные сети и сетевая безопасность (M.Sin Computer Science – Computer Networks and Network Security); -Магистр компьютерных наук – Компьютерные сети и безопасность (M.Sin Computer Science – Computer Networks and Security); -Магистр систем вычислительной техники (M.Sin Computer Systems Engineering - Computer Networks and Network Security); -Магистр телекоммуникаций и компьютерных сетей–Безопасность (M.S in Telecommunications and Networking – Security); -Магистр компьютерной, информационной и сетевой безопасности–специализация–Управление рисками (M.S. in Computer, Information and Network Security - Governance, Risk and Compliance Concentration)
5. Управление информационной безопасностью.	-Магистр безопасности информационных технологий и управления– профессиональный уровень (M.S. in Information Security Technology and Management - Professional Track) -Магистр безопасности информационных технологий и управления – научно-исследовательский уровень (M.S. in Information Security Technology and Management – Research Track); - Магистр информационных технологий – Специализация – управление информационной безопасностью (M.S. in Information Technology With Concentration in Information Security Management)

## ПРИЛОЖЕНИЕ Г

**Учебный план образовательной программы «Информационная безопасность»  
(магистратура) колледжа Мерси**

Таблица Д.1 – Учебный план образовательной программы «Информационная безопасность» (магистратура) колледжа Мерси. Специализированные дисциплины по направлению ИБ.

Дисциплина (модуль)	Описание
<b>Введение в информационную безопасность</b>	<p><b>Цели и задачи дисциплины:</b> курс дает широкий взгляд на обеспечение информационной безопасности.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-защита информационных ресурсов;</li> <li>-доступ к информационной системе,</li> <li>-незаконный доступ, взлом;</li> <li>-законодательство в области информационной безопасности;</li> <li>-промышленные стандарты</li> </ul>
<b>Расследование компьютерных инцидентов</b>	<p><b>Цели и задачи дисциплины:</b> курс рассматривает вопросы, связанные с компьютерной криминалистикой. Теоретический материал прямо коррелирует с практическими методами.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-основные понятия, используемые в компьютерной экспертизе;</li> <li>-методы, необходимые для проведения судебной экспертизы компьютерных систем и данных;</li> <li>-требования к восстановлению данных;</li> <li>-исследования компьютерного мошенничества.</li> </ul> <p><b>Формы работы:</b> лекции и практические упражнения</p>
<b>Межсетевые экраны и обнаружение вторжений (Firewall and Intrusion Detection),</b>	<p><b>Цели и задачи дисциплины:</b> дисциплина знакомит понятием брандмауэра и системы обнаружения вторжения.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-основные правила настройки;</li> <li>-выбор технологии брандмауэра;</li> <li>-основные рекомендации по установке брандмауэра;</li> <li>-типы вторжений;</li> <li>-системы обнаружения вторжений, блокирование вторжений</li> </ul> <p><b>Формы работы:</b> лекции и практические упражнения по тестированию и оценки надежности различных методов брандмауэра</p>
<b>Безопасность беспроводных сетей</b>	<p><b>Цели и задачи дисциплины:</b> дисциплина знакомит с различными беспроводными технологиями, беспроводными сетями, обсуждаются риски безопасности и управление рисками.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-сетевые протоколы;</li> <li>-режимы доступа;</li> <li>-беспроводные устройства;</li> <li>-средства управления;</li> <li>-угрозы безопасности</li> </ul>
<b>ИТ-аудит</b>	<p><b>Цели и задачи дисциплины:</b> Дисциплина рассматривает важнейшие навыки и методы, используемые для обеспечения соответствия нормативным требованиям в государственном и частном секторах.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-внутренние и внешние требования аудита;</li> <li>-обеспечение надлежащего уровня контроля;</li> <li>-контроль на уровне технологий и на уровне процессов</li> </ul>

Дисциплина (модуль)	Описание
<b>Социальные аспекты информационной безопасности</b>	<p><b>Цели и задачи дисциплины:</b> дисциплина рассматривает социальные последствия информационной безопасности.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-социальные воздействия современной вычислительной техники;</li> <li>-правовые вопросы современной вычислительной техники;</li> <li>-вопросы интеллектуальной собственности;</li> <li>-профессиональные и этические проблемы и обязанности;</li> <li>-конфиденциальность и гражданские свободы</li> </ul>
<b>Данные и интеллектуальный анализ</b>	<p><b>Цели и задачи дисциплины:</b> Дисциплина знакомит с последними разработками в интеллектуальном анализе данных.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-подготовка данных;</li> <li>-оценка данных;</li> <li>-кластеризации и классификации;</li> <li>-практические методы, используемые в области анализа данных</li> </ul>
<b>Безопасность распределенных баз данных</b>	<p><b>Цели и задачи дисциплины:</b> Дисциплина, посвящена защите баз данных и методам защиты распределенных данных.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-обязательный контроль доступа;</li> <li>-проектирование защищенной базы данных;</li> <li>-целостность данных;</li> <li>-безопасная архитектура;</li> <li>-безопасная обработка транзакций;</li> <li>-информационный поток управления и вывод контроля</li> </ul>
<b>Безопасность электронной коммерции</b>	<p><b>Цели и задачи дисциплины:</b> Дисциплина знакомит с современными угрозами, стоящими перед организациями, которые осуществляют бизнес в Интернете. Рассматриваются вопросы по решению данных проблем.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-обзор криптографии,</li> <li>-сертификаты безопасности,</li> <li>-безопасные услуги на основе учетных данных и авторизации на основе ролей,</li> <li>-мобильный код безопасности;</li> <li>-безопасность систем клиента;</li> <li>-защищенные электронные транзакции;</li> <li>-электронные платежные системы;</li> <li>-защита интеллектуальной собственности;</li> <li>-вопросы права и регулирования</li> </ul>
<b>Политика информационной безопасности</b>	<p><b>Цели и задачи дисциплины:</b> дисциплина, посвящена объяснению политик безопасности, которые играют важную роль в надежных системах безопасности.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-создание политики информационной безопасности;</li> <li>-процедуры и стандарты;</li> <li>-использование принятых правил;</li> <li>-соблюдения и обеспечения выполнения политики безопасности</li> </ul>
<b>Прикладная криптография</b>	<p><b>Цели и задачи дисциплины:</b> дисциплина дает полное представление о криптографии.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-общая концепция безопасности;</li> <li>-безопасность связи, в том числе криптографии;</li> <li>-различия между асимметричными и симметричными типами алгоритмов;</li> <li>-PKI сертификаты и их использование</li> </ul>

Дисциплина (модуль)	Описание
<b>Практические вопросы безопасности</b>	<p><b>Цели и задачи дисциплины:</b> Формирование практических навыков в области защиты информации в конкретной организации</p> <p><b>Содержание:</b> Защита информации по отраслям экономики: -здравоохранение; -государственное управление; -финансовые организации; -образование и наука и проч.</p> <p><b>Формы работы:</b> работа по индивидуальному плану</p>
<b>Специальные вопросы информационной безопасности</b>	<p><b>Цели и задачи дисциплины:</b> в рамках дисциплины изучаются прототипы, тенденции будущего развития систем и методов в области информационной безопасности</p>
<b>Независимые исследования</b>	<p><b>Цели и задачи дисциплины:</b> в рамках дисциплины студенты проводят независимые исследования в области информационной безопасности под руководством преподавателя</p>

## ПРИЛОЖЕНИЕ Д

## Учебный план образовательной программы «Корпоративная и информационная безопасность»

Таблица Е.1 – Учебный план образовательной программы. «Дисциплины первого этапа обучения, связанные с ИБ. Некоторые обязательные дисциплины второго этапа обучения, связанные с ИБ»

Дисциплина (модуль)	Описание
Производственная практика по информационной практике	<p><b>Цели и задачи дисциплины:</b> формулирует принимающая сторона</p>
Проектные работы (практика)	<p><b>Цели и задачи дисциплины:</b> применение теоретических и практических знаний при реализации сложных проектов в профессиональной среде и практико-ориентированных командах.</p> <p><b>Содержание:</b> практическое управление безопасностью в контексте реальных проблем в корпоративном поле</p> <p><b>Формы работы:</b> практика</p> <p><b>Формы контроля:</b> практическая работа (проектные работы)</p>
Диссертация	<p><b>Цели и задачи дисциплины:</b> показать умение самостоятельного решения определенной проблемы информационной безопасности на основе полученных теоретических и практических знаний и с использованием научных методов.</p> <p><b>Содержание:</b> -подробная разработка предложенной темы, включает теоретические разработки и практическую часть; -составление 80-страничной документации. Она должна охватывать все основные аспекты дипломной работы и быть написана в соответствии с научными критериями; -презентация и защита результатов во время коллоквиума</p> <p><b>Формы работы:</b> самостоятельная разработка темы</p> <p><b>Формы контроля:</b> презентация и защита диссертации</p>



Таблица Е.2 – Учебный план образовательной программы. Дополнительные дисциплины второго этапа обучения.

Дисциплина (модуль)	Описание
<b>Обратное проектирование</b>	<p><b>Цели и задачи дисциплины:</b> дать простые понятия и методы обратного проектирования для выявления уровня безопасности программных средств.</p> <p><b>Содержание:</b> -дизассемблеры, отладчики и декомпиляторы; -функциональность машинного языка, машинный код для x86 процессоров, использование ассемблера; -использование обратного проектирования для устранения неисправностей, защиты от копирования, восстановления исходной программы, защита от исследования кода; -введение в обратное проектирование программного обеспечения.</p> <p><b>Формы работы:</b> лекции и лабораторные занятия.</p> <p><b>Формы контроля:</b> письменный экзамен, лабораторные работы (лабораторный практикум обратное проектирование)</p>
<b>Тестирования на проникновение</b>	<p><b>Цели и задачи дисциплины:</b> -научить применять процедуры и методы для анализа современных ИТ-инфраструктур, операционных систем и приложений; -научить применять сложные методы и инструменты для профессионального анализа и консультаций в области информационной безопасности;</p> <p><b>Содержание:</b> -организация проверок безопасности и реализации концепции тестирования на проникновение; белый, серый и черный ящик; -анатомия атаки, цель проникновения, расширенный поиск в Google, отпечаток системы, приложений и сетей, сканирование портов, пассивный и активный поиск информации, обнаружение и обход брандмауэра, отказ в обслуживании; -анализ уязвимостей, внешних и внутренние угрозы проникновения по сети, фаззинг, подбор пароля перебором, эксплуатация уязвимостей, эксплуатация хакерских утилит типа Metasploit; -анализ проникновения, результаты тестирования и документация; -тестирование на проникновение Стандарты ISO / IEC 27001 / 2, OSTTMM (Open Source Security Test Methodic Manual), OWASP (Open Web Application Security Project) и LPT (License Tester Penetration)</p> <p><b>Формы работы:</b> лекции и лабораторные занятия</p> <p><b>Формы контроля:</b> письменный экзамен, и лабораторные работы (лабораторный практикум тестирование на проникновение)</p>
<b>Разработка безопасных web приложений (специализация-разработка безопасных приложений)</b>	<p><b>Цели и задачи дисциплины:</b> анализ и проектирование безопасных веб-приложений</p> <p><b>Содержание:</b> -серверы и клиенты в сети, 3-х уровневая архитектура; -атаки на веб-приложения, XSS, черви, безопасность; ActiveX, Java и PHP; -DoS и DDoS-атаки, WebSecurity сканер; -защита от веб-атак</p>
<b>Практика Приложения для предприятий (специализация-разработка)</b>	<p><b>Цели и задачи стажировки:</b> -анализ и проектирование программной архитектуры предприятия; - возможности и ограничения корпоративных приложений; -решение проблемы масштабируемости программных систем;-внедрение новых технологий</p> <p><b>Содержание:</b></p>

Дисциплина (модуль)	Описание
<b>безопасных приложений)</b>	<p>-60 ч работа на предприятии;  -60 ч самостоятельной работы (например, программирование);  -30 часов подготовка к защите</p> <p><b>Формы контроля:</b>  модульный  защита практики «Приложения для предприятий»</p>
<b>Конкурентная разведка (специализация-безопасность предприятия)</b>	<p><b>Цели и задачи дисциплины:</b>  оценка уровня конкуренции и анализ рынка, с учетом связанных с этим этических и юридических аспектов</p> <p><b>Содержание:</b>  -бизнес и маркетинг;  -конкурентная разведка как стратегический подход;  -СІ-цикл;  -источники данных;  -аналитические методы и стратегическое управление;  -организационная интеграция СІ</p> <p><b>Формы работы:</b>  лекции, лабораторные занятия и семинары</p> <p><b>Формы контроля:</b>  -письменный экзамен, лабораторные работы (конкурентная разведка);  -защита проекта практики “Конкурентная разведка”</p>
<b>Предупреждение и управление в кризисных ситуациях(специализация-безопасность предприятия)</b>	<p><b>Цели и задачи обучения:</b>  -планирование и осуществление мер готовности к чрезвычайным ситуациям;  -антикризисное управление организации;  -определение критических и ноу-хау областей в работе компании;  -применение профилактических мер против промышленного шпионажа и манипуляций персоналом</p> <p><b>Содержание:</b>  -кризис управления, как организационная задача;  -информация и коммуникация в условиях кризиса;  -подготовка и осуществление кризисных планов;  -ранняя диагностика кризисных явлений в корпоративной среде;  -критические области бизнеса;  -сценарий атаки на корпоративную информацию;  -контрразведки</p> <p><b>Формы работы:</b>  лекции</p> <p><b>Формы контроля:</b>  -письменный экзамен;  -практическая работа (управления в кризисных ситуациях, контрразведка и профилактика шпионажа)</p>

## ПРИЛОЖЕНИЕ Е

Учебный план образовательной программы «Компьютерные науки (ИБ)»  
(бакалавриат) в Боннском университете

Таблица Ж.1 – Учебный план образовательной программы «Компьютерные науки (ИБ)»  
(бакалавриат) в Боннском университете. Обязательные дисциплины, связанные с ИБ

Дисциплина (модуль)	Описание
Информационная безопасность	<p><b>Цели и задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>-дать основные требования, концепции и методы защиты информации;</li> <li>-дать теоретические и практические знания в области информационной безопасности и сетевой безопасности;</li> </ul> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- анализ угроз, анализ рисков, политика безопасности;</li> <li>-основные меры защиты. Общие критерии;</li> <li>-основы криптографических методов: шифрование, криптографические хеш-функции, коды обнаружения модификации, коды аутентификации, цифровая подпись;</li> <li>-введение в криптографические протоколы;</li> </ul> <p>Сетевая безопасность:</p> <ul style="list-style-type: none"> <li>-атаки на информационные системы, TCP/IP протокол;</li> <li>-межсетевой экран: пакетные фильтры, прокси-фильтры сеансового уровня, прокси на уровне приложений, архитектура брандмауэра, обнаружение вторжений, безопасность брандмауэра;</li> <li>-IP Security: безопасность для задач и приложений, режим транспорта и туннельный режим защищенной связи, политики безопасности баз данных, аутентификация, инкапсуляции безопасности полезной нагрузки, управление ключами, интернет-ключи, протокол обмена ключами и сертификатами Деффи-Хелмана, протокол Фотурис и другие протоколы;</li> <li>-протокол «Secure Socket Layer»: Уровень SSL, SSL обмен данными, отличия от TLS, открытый ключ инфраструктур, OpenSSL</li> </ul> <p>Безопасность операционных систем:</p> <ul style="list-style-type: none"> <li>-идентификация и аутентификация, управление доступом, контрольный монитор;</li> <li>-разработка защищенного ПО</li> </ul> <p><b>Формы работы:</b></p> <ul style="list-style-type: none"> <li>-лекций и панельные студенческие дискуссии.</li> <li>-практические упражнения с возможностью саморедактирования.</li> <li>-самостоятельная работа в небольших группах (три студента) по обработке практических задач сетевой безопасности.</li> <li>-обучение на основе платформы Moodle: дискуссии, примеры решений, контроль качества освоения лекций и упражнений.</li> </ul> <p><b>Формы контроля:</b></p> <p>письменный экзамен. Независимое решение упражнений. Успешная работа в группе</p>
Электронные ключи	<p><b>Цели и задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>-дать теоретические и практические основы использования электронных ключей безопасности, их технологического устройства;</li> <li>-разработка студентами на основе электронных ключей компонентов криптографических систем.</li> </ul> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-протоколы безопасности для электронных ключей: ключевой метод соглашения, методы аутентификации (симметричные, асимметричные), пароль на основе криптографических алгоритмов, анонимные / псевдоанонимные методы аутентификации</li> </ul> <p><b>Формы контроля:</b></p> <p>Экзамен (устный или письменный). Независимое решение упражнений</p>

Дисциплина (модуль)	Описание
<b>Прикладная криптография</b>	<p><b>Цели и задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>- дать теоретические и практические основы современной криптографии, как симметричных так и с открытым ключом методов;</li> <li>- выработать навыки программной разработки криптографических алгоритмов для информационных технологий и телекоммуникаций</li> </ul> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- введение в криптографию и криптоанализ, исторические шифры;</li> <li>- теория крипто систем;</li> <li>- поточные шифры: Псевдо генераторы случайных чисел, одноразовый блокнот, LFSRs, потоковые шифры на основе LFSRs, другие потоковые шифры, методы криптоанализа;</li> <li>- блочные шифры: принципы работы, режимы работы (ECB, CBC, CFB, OFB, CNT), DES, AES, методы криптоанализа;</li> <li>- хэш-функции: основы, хэш-функций на основе семейства MD4 (SHA-1), последняя реализация SHA-3, методы криптоанализа;</li> <li>- проблемы теории чисел;</li> <li>- криптосистем с открытым ключом на основе факторинга (RSA) и дискретного логарифмирования (Эль-Гамаль);</li> <li>- ЭЦП, RSA, Шнорра, DSA</li> </ul> <p><b>Формы работы:</b></p> <p>обучение на основе платформы Moodle: дискуссии, примеры решений, контроль качества освоения лекций и упражнений. лекции, теоретические задачи, практические упражнения.</p> <p><b>Формы контроля:</b></p> <p>экзамен (письменный или устный). Независимое решение упражнений</p>
<b>Безопасность мобильных устройств</b>	<p><b>Цели и задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>- дать теоретические и практические основы стандартов безопасности для мобильных систем;</li> <li>- выработать навыки применения стандартов безопасности для мобильных систем, различных сетей связи и ИТ-инфраструктуры</li> </ul> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- системы виртуализации, LFS;</li> <li>- хостинг контроля доступа и мониторинга / аудита;</li> <li>- механизмы защиты и шифрования дисков;</li> <li>- системы обнаружения / предотвращения вторжений (IDS / IPS);</li> <li>- безопасный беспроводной доступ (WEP, WPA, WPA-2);</li> <li>- протоколы безопасного удаленного доступа 802.1X, AAA Framework Горячие точки</li> <li>- протоколы безопасности IPv6, Mobile IP;</li> <li>- безопасность в беспроводных сетях (Bluetooth, GSM, UMTS)</li> </ul> <p><b>Формы работы:</b></p> <p>лекций, самостоятельная работа в небольших группах (три студента) по отработке практических заданий по настройке мобильных систем и настройке безопасных беспроводных сетей в соответствии со стандартами безопасности.</p> <p><b>Формы контроля:</b></p> <p>экзамен (письменный или устный)</p>
<b>Управление информационной безопасностью</b>	<p><b>Цели и задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>- дать теоретические знания в области угроз информационной безопасности, последствий ущерба, возможных технических и организационных мер.</li> <li>- научить студентов применять методы управления в области информационной безопасности, оценивать экономические затраты</li> </ul> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>- определения терминов, стандартов и других нормативных актов;</li> <li>- основные категории безопасности;</li> <li>- оценка риска;</li> <li>- инструкции по безопасности;</li> <li>- организация информационной безопасности;</li> <li>- управление собственным ценностям организации;</li> <li>- личная безопасность;</li> <li>- физическая и экологическая безопасность;</li> </ul>

Дисциплина (модуль)	Описание
	<ul style="list-style-type: none"><li>-операционный и коммуникационный менеджмент;</li><li>-управление доступом;</li><li>-закупка, разработка и сопровождение информационных систем;</li><li>-работа с инцидентами информационной безопасности;</li><li>-обеспечение бизнес-операций (управление непрерывностью бизнеса);</li><li>-соответствие нормативным требованиям и стандартам.</li></ul> <p><b>Формы работы:</b> лекции, самостоятельная работа в небольших группах (три студента) с использованием различных электронных систем, таких как Moodle и Wiki</p> <p><b>Формы контроля:</b> презентация промежуточных результатов, экзамен (письменный или устный)</p>

## ПРИЛОЖЕНИЕ Ж

### Учебный план образовательной программы «Управление безопасностью» (магистратура) Университета прикладных наук города Бранденбурга

Таблица И.1 Учебный план образовательной программы «Управление безопасностью» (магистратура) Университета прикладных наук города Бранденбурга. Дисциплины первого семестра обучения, связанные с управлением безопасностью.

Дисциплина (модуль)	Описание
<b>Основы управления безопасностью</b>	<p><b>Цели и задачи дисциплины:</b>  обзор корпоративной безопасности;  -создание бизнес-кейсов по вопросам безопасности;  - оценка рисков и рассмотрение угроз, показатели эффективности и их стоимость.  -понимание роли "доверенного советника".</p> <p><b>Содержание:</b>  -что такое безопасность технологий и поведенческая психология злоумышленников;  -управление рисками;  -управление безопасностью как процесс обеспечения управления (инциденты, кризисы и стихийные бедствия, регулирование кризисов и обеспечение непрерывности бизнес процессов, безопасность отчетности);  -отдел безопасности;  -требования и критерии сотрудников для управления безопасностью;  -архитектура безопасности непрерывности бизнес-процессов;  -физическая безопасность-CERT;  -безопасность операционных систем и программного обеспечения;  -защита от видео- и аудио- наблюдений</p> <p><b>Формы работы:</b>  лекции с презентациями, кратковременная (1-2 занятие) работа над задачами и мини-проектами в малых группах (3 человека), ролевые игры, индивидуальные презентации.</p> <p><b>Особенности:</b>  преобладание динамической работы в группах.</p> <p><b>Форма контроля:</b>  презентация и доклад, защита предложенных бизнес-проектов, письменное резюме.</p>
<b>Безопасность сети</b>	<p><b>Цели и задачи дисциплины:</b>  курс дает практическое понимание безопасности IP-сетях связи;  -анализ рисков, связанных с эксплуатацией уязвимостей в приложениях и протоколах;  -показать на практических примерах процессы и стратегии сетевых атак, методы безопасной эксплуатации сетевых компонентов.</p> <p><b>Содержание:</b>  -основы Интернета (TCP / IP протокол, ISO / OSI модель, активные компоненты, криптография, категории угроз, уязвимости, управление безопасностью, аудит безопасности с помощью инструментов, мониторинг сети и сетевых регистраций, атак и контрмеры);  -криптография (шифрование переписки, VPN соединения, сертификаты);  -веб- безопасность, безопасность электронной почты (практическое применение брандмауэров, Nonneurop)</p> <p><b>Формы работы:</b>  лекции, практические занятия по конкретным темам из лекций</p> <p><b>Форма контроля:</b> проектная работа по выбранному модулю</p>

Дисциплина (модуль)	Описание
<b>Основы безопасности коммуникационных технологий</b>	<p><b>Цели и задачи дисциплины:</b>            дать основные знания по методам и сценариям нападения и защиты, оценке и разработке собственной системы безопасности;            -познакомить с рядом программно-аппаратных средств безопасности.</p> <p><b>Содержание:</b>            -компоненты систем безопасности (электронные ключи, хранение и управление ключами; возможности и ограничения электронной связи; модели косвенных/прямых атак через каналы связи, основные понятия и разработка критериев);            -компоненты встраиваемых систем (модели угроз, безопасность элементов и механизмов, жизненный цикл и управление устройствами);            -смарт-карты (виды, типы, характеристики, жизненный цикл в производственном процессе, программирование и внедрение; модели угроз и атак, несанкционированный доступ к чипу, концепции доверия)</p> <p><b>Формы работы:</b>            лекция с презентациями, практика в компьютерном классе в небольших группах (до 10 человек)</p> <p><b>Форма контроля:</b>            экзамен с практическим заданием по экспертизе компонентов связи</p>
<b>Криптология</b>	<p><b>Цели и задачи дисциплины:</b>            дать студентам математические основы безопасной передачи информации, теории информации, криптографии и криптоанализа;            -дать навыки работы с криптографическими приложениями.</p> <p><b>Содержание:</b>            Лекции:            -методы обеспечения секретности, безопасности и целостности;            -подлинность электронных коммуникаций;            -общие протоколы шифрования и оценка их сильных и слабых стороны;            -методы обеспечения безопасной электронной коммерции</p> <p>практические занятия:            использование криптографических приложений;            методы криптоанализа</p> <p>курсовая работа по криптологии</p> <p><b>Формы работы:</b>            лекция с презентациями, практика в компьютерном классе в небольших группах (до 10 человек).</p> <p><b>Форма контроля:</b>            экзамен с практическим заданием</p>
<b>Курсовая работа</b>	<p><b>Цели и задачи дисциплины:</b>            закрепление и расширение способности студентов к самостоятельной научной работы в области управления безопасностью;            -подготовка практической части магистерской диссертации.</p> <p><b>Содержание:</b>            первичное обследование (сбор статистики, интервью, первичных / вторичных источников), сбор источников по теме исследования, определение требований к стилю (реклама, пресс-релизы, научная работа), сбор материалов и проведение исследований, анализ результатов.</p> <p><b>Формы работы:</b>            работа в малых группах</p> <p><b>Форма контроля:</b>            защита курсовой работы</p>
<b>Дисциплина по выбору</b>	<p><b>Цели и задачи дисциплины:</b>            дать студентам представление о контекстах, прилегающих к области управления безопасностью.</p> <p><b>Содержание:</b>            -глобальная безопасность;            -безопасность промышленности;            -безопасность мобильных ИТ-решений;            -конфиденциальность, защита от неправильного обращения, критическая</p>

Дисциплина (модуль)	Описание
	<p>инфраструктура;  -сертификация;  -риски и защита от мошенничества;  -социальная инженерия;  -ликвидация последствий стихийных бедствий;  -риски культуры;  -компьютерная преступность;  -тематические исследования</p> <p><b>Формы работы:</b>  лекции с презентациями</p> <p><b>Форма контроля:</b>  студенческая конференция, коллоквиум</p>

Таблица И.2 – Учебный план образовательной программы «Управление безопасностью» (магистратура) Университета прикладных наук города Бранденбурга. Дисциплины второго семестра обучения.

Дисциплина (модуль)	Описание
<p><b>Безопасность и регулирование кризисов. Международный контекст</b></p>	<p><b>Цели и задачи дисциплины:</b>  углубление знаний, полученных по дисциплине управление безопасностью</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-архитектура, инструменты, процессы;</li> <li>-мошенничество и расследование инцидентов;</li> <li>-управление безопасностью в глобальных организациях;</li> <li>-разработка безопасного программного обеспечения;</li> <li>-работа отдела по блокированию внешних воздействий на систему безопасности</li> </ul> <p><b>Формы работы:</b>  лекции с презентациями, разработка идей в малых группах, мини-проекты, ролевые игры, индивидуальные презентации.</p> <p><b>Форма контроля:</b>  финальный отчет по разработке группового проекта (ролевой игры)</p>
<p><b>Рабочее место специалиста по управлению безопасностью</b></p>	<p><b>Цели и задачи дисциплины:</b>  дать студентам методологические и технологические основы защиты и техники безопасности, действий при стихийных бедствиях, механических устройств безопасности, системы сигнализации и контрольного оборудования. Область применения и ограничения систем безопасности, доступных на рынке. Большое внимание уделяется изучению правовой базы по использованию механизмов безопасности.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-рабочее место специалиста (обзор задач и возможностей, технические основы, физические атаки, модель злоумышленника - цели и методы нападения, использование электронных устройств);</li> <li>-механические устройства безопасности и контроля доступа (замки, системы запирающие и их безопасность, защита от проникновения через двери, окна и заборы, сейфы и шкафы, технические и правовые нормы и директивы);</li> <li>-охранные системы (основы, системы охранной сигнализации, противопожарная и пожаротушения системы, технические и правовые нормы и директивы);</li> <li>-мониторинг объектов (технические возможности, явные и скрытые наблюдения, технические и юридические правила и нормы);</li> <li>-планирование чрезвычайных ситуаций</li> </ul>



Дисциплина (модуль)	Описание
<b>Управление сетевой безопасностью</b>	<p><b>Цели и задачи дисциплины:</b></p> <p>Сформировать навыки применения методов, моделей атак и механизмов защиты, развить глубокое понимание фундаментальных проблем корпоративной ИТ-безопасности;</p> <p>-привести данные о модели безопасности и политики безопасности, управлении ключами, компьютерной экспертизе и оценки ИТ-систем безопасности.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-защита данных;</li> <li>-архивирование системы;</li> <li>-аварийное восстановление;</li> <li>-модели безопасности;</li> <li>-модель контроля доступа и модель информационных потоков (руководящие принципы использования);</li> <li>-управление ключами в сетевой инфраструктуре (сертификаты, сертификация, сертификация и РКІ, генерация ключей, хранение, восстановление ключей, обмен ключами);</li> <li>-политика безопасности и их реализация (правоприменение, механизмы безопасности, обнаружение и предотвращение вторжений, компьютерная экспертиза, защищенная компьютерная система, управление цифровыми правами);</li> <li>-оценка ИТ-систем безопасности (критерии оценки ИТ-систем и инфраструктуры, базовая защита, общие критерии)</li> </ul> <p><b>Формы работы:</b></p> <p>лекции с презентациями, практика в компьютерном классе в небольших группах (до 10 человек)</p> <p><b>Форма контроля:</b></p> <p>экзамен с практическим заданием</p>
<b>Развитие безопасных ИТ-систем</b>	<p><b>Цели и задачи дисциплины:</b></p> <p>дать знания о методах применения защитных требований, анализе угроз и разработке ИТ-систем, создание и внедрение политик безопасности и архитектур безопасности;</p> <p>-привести методы и инструменты для разработки программного обеспечения для использования в критически важных областях;</p> <p>-дать студентам практическое понимание современных методов проектирования безопасности критически важных ИТ-приложений.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-разработка программного обеспечения, программирование и аппаратное обеспечение;</li> <li>-фаза моделирования и принципы проектирования (структурный анализ и оценка потребностей, анализ рисков, стратегия безопасности, проверка архитектуры безопасности);</li> <li>-безопасность внедрения ИТ-системы (программная ошибка как угроза безопасности, вопросы безопасности в программировании, языки программирования и операционные системы, средства разработки, проектирование интерактивных ИТ-систем безопасности, взаимодействие человека с компьютером);</li> <li>-оценка ИТ-систем безопасности (методы испытаний и процедуры, неформальные и формальные проверки ИТ-систем)</li> </ul> <p><b>Формы работы:</b></p> <p>Лекции с презентациями, практика в компьютерном классе в небольших группах (до 10 человек), самостоятельная работа</p> <p><b>Форма контроля:</b></p> <p>Устный экзамен;</p> <p>-практическая работа (создание безопасного программного обеспечения)</p>

Дисциплина (модуль)	Описание
Управление персоналом	<p><b>Цели и задачи дисциплины:</b></p> <p>ознакомить студентов с новейшими методами корпоративного управления. Особое внимание уделяется рассмотрению критических ситуаций в бизнесе и разрешению конфликтов.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-функции управления (бизнес-цели, принципов, культуры, разработка стратегий, кадры и собеседование, международные аспекты глобальной конкуренции);</li> <li>-этические аспекты корпоративного управления (стратегия борьбы с коррупцией, кодекс поведения и т.д.);</li> <li>-управление рисками;</li> <li>-антикризисное управление (теория корпоративных кризисов, методы признания кризиса, антикризисное управление, правовые нормы);</li> <li>-управление конфликтами (конфликт, виды конфликтов, эскалация, стратегия управления конфликтами)</li> </ul> <p><b>Формы работы:</b></p> <p>лекции с поддержкой тематических исследований и/или имитационной игры; лекции приглашенных докладчиков на основе соответствующих практических примеров. Работа над проектом, ролевые игры.</p> <p><b>Форма контроля:</b></p> <p>устный экзамен; -защита проектной работы.</p>
Производственная практика	<p><b>Цели и задачи дисциплины:</b></p> <p>дать студентам знания по научной работе с мультиконтекстной проблемой на производстве.</p> <p>Проект 1 “Интернет преступность” (вирусы, черви, нежелательный контент, онлайн-мошенничество, нарушения конфиденциальности).</p> <p>Проект 2 “Прикладные системы” (выбор, конфигурация и настройка прикладного программного обеспечения для предприятия).</p> <p>В рамках проекта студенты для реальных компаний и организаций представляют научно аргументированные документированные практические результаты.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-постановка проблемы (состояние, интеграция в существующую практику, использование различных методов анализа - интервью, анкета, метод Делфи, анализ документов);</li> <li>-анализ уязвимостей (сравнение приложений, научно обоснованное развитие практического подхода, использование творческих методов, затраты и экономическая эффективность);</li> <li>-разработка прототипа (прототип реализации, разработка программного прототипа);</li> <li>-внедрение в компании / организации</li> </ul> <p><b>Формы работы:</b></p> <p>проектная работа в группах до 7 человек в компании / организации.</p> <p><b>Форма контроля:</b></p> <p>Отчет по проекту, защита практики с представителями компаний / организаций</p>

Таблица И.3 – Учебный план образовательной программы «Управление безопасностью» (магистратура) Университета прикладных наук города Бранденбурга. Дисциплины третьего семестра обучения.

Дисциплина (модуль)	Описание
Дисциплины по выбору	<p><b>Цели и задачи дисциплины:</b></p> <p>факультативы создаются для раскрытия практических вопросов управления безопасностью в компаниях и организациях.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-управление безопасностью: системы управления, компьютерная экспертиза, киберпреступность, борьба со стихийными бедствиями, персонал и охранники, аудит безопасности, безопасность консалтинга и т.д.;</li> <li>-безопасность при передаче голоса по IP (VoIP) (применение VOIP, анонимность, конфиденциальность данных, мошенничество, соблюдение информации безопасность);</li> <li>-практическое тестирование (разработка контрольных перечней концепции безопасности)</li> </ul> <p><b>Формы работы:</b></p> <p>лекции, практическая работа в малых (2 участника) группах., работа в компании/организации</p> <p><b>Форма контроля:</b></p> <p>защита практических работ</p>
Мастер-семинар	<p><b>Цели и задачи дисциплины:</b></p> <p>дать навыки обработки результатов проекта и написания научной работы. Стандарты международных исследований</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-передовые научные методы;</li> <li>-стандарты научной работы;</li> <li>-введение в международное документоведение;</li> <li>-экспертиза научных работ;</li> <li>-методам научного рецензирования</li> </ul> <p><b>Формы работы:</b></p> <p>презентации, активное участие студентов в дискуссии и рабочих группах</p> <p><b>Форма контроля:</b></p> <p>без оценки</p>
Магистерская диссертация	<p><b>Цели и задачи дисциплины:</b></p> <p>показать теоретические и практические знания, способность самостоятельно работать в области “Управление безопасностью”</p> <p><b>Содержание:</b></p> <p>время работы над диссертацией составляет 4 месяца. Тема магистерской диссертация связана с исследованием теоретической или практической проблемы. Объем магистерской диссертации не менее 60 страниц.</p> <p><b>Формы работы:</b></p> <p>самостоятельная научная работа</p> <p><b>Форма контроля:</b></p> <p>защита магистерской работы (3/4 оценки ставиться за результаты работы, 1/4 оценки ставиться за выступление)</p>

## ПРИЛОЖЕНИЕ И

### Учебный план образовательной программы «Компьютерная безопасность» (магистратура) университета в городе Лимож

Таблица К.1 – Учебный план образовательной программы «Компьютерная безопасность» (магистратура) университета города Лимож. Дисциплины первого года обучения, связанные с ИБ.

Дисциплина	Описание
<b>Введение в криптологию</b>	<p><b>Цель:</b> дать студентам основы криптографии</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-основы криптографии: проблемы;</li> <li>-теория информации, энтропия;</li> <li>-криптоанализ исторических систем;</li> <li>-безопасность услуг, криптографическая аутентификация, целостность, конфиденциальность, доказательство;</li> <li>-принципы криптографии: диффузия, спутанность сознания, Kerckhoffs принцип;</li> <li>-секретный ключ шифрования, блочные шифры и потоковые шифры, DES/3DES, AES, RC4, хэш-функция SHA-1;</li> <li>-открытый ключ шифрования: секретный обмен, RSA, Диффи-Хеллмана, Эль-Гамала, эллиптические кривые;</li> <li>-криптографическая аутентификация, MAC, криптографические принципы электронных подписей;</li> <li>-проблема распределения, управления и защиты ключей</li> </ul>
<b>Информационная безопасность</b>	<p><b>Цель:</b> дать понятия о безопасном использовании связи, Интернета и информационных технологий и связи.</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-защита отдельных рабочих станций: защита электронных документов, защита от «вредоносных» программ (вирусы, шпионские программы, руткиты), персональные брандмауэры;</li> <li>-управление доступом, основные методы аутентификации, пароль;</li> <li>-использование электронной подписи, цифровые сертификаты;</li> <li>-Communications Security: электронная почта, Интернет, удаленный доступ к интернет-сайтам;</li> <li>-защита конфиденциальности: трассировка соединений, программ-шпионов</li> </ul>
<b>Компьютерные сети</b>	<p><b>Цель:</b> дать студентам знания об основах сетей и их безопасности</p> <p><b>Содержание:</b></p> <ul style="list-style-type: none"> <li>-низкоуровневое сетевое программирование: Использование выделенных виртуальных платформ (VMware, VirtualBox); Разработка инструментов для анализа трафика;</li> <li>-управление трафиком в сетях: управление трафиком приложений, Межсетевой экран;</li> <li>-риски, связанные с фильтрацией и ограничениями: грубая сила, фрагменты, SYN Cookie;</li> <li>-QoS управление потоком;</li> <li>-виртуальные частные сети: развертывание и применение: протоколы для безопасного доступа к сети (EAP, 802.1X, Radius); IPSec, OpenVPN, сертификаты;</li> <li>-IPv6 развертывания и конфигурирования.</li> </ul>

Таблица К.2 – Учебный план программы «Компьютерная безопасность» (магистратура) университета образовательной города Лиможа. Дисциплины второго года обучения, связанные с ИБ

Дисциплина	Содержание
<b>Шифрование секретным ключом</b> с	<ul style="list-style-type: none"> <li>-Фейстеля схема, режим цепочки, линейный и дифференциальный криптоанализ;</li> <li>-Анализ и проектирование хэш-функций. Итерационные функции;</li> <li>-Атаки: multicollisions, длинные сообщения, сообщения масштабируемости, атаки на SHA-1, MAC: HMAC, CBC-MAC, конкретные атаки;</li> <li>-Псевдослучайные генераторы: криптографическая защита, проектирование и криптоанализ</li> </ul>
<b>Криптография открытым ключом</b> с	<ul style="list-style-type: none"> <li>-Безопасность схемы с открытым ключом: RSA эквивалент секретных данных, семантика безопасности, RSA значимые биты, безопасные биты, атака на участников обмена, проблема эквивалентности;</li> <li>-Сертификат безопасности;</li> <li>-Криптоалгоритмы: с нулевым знанием, Fiat-Shamir, Шнорра, GQ, PIZK;</li> <li>-Генераторы случайных чисел: BBS, безопасность в RQ;</li> <li>-Криптосистемы и атаки: XTR, NTRU, HFE</li> </ul>
<b>Криптографические механизмы и приложения</b>	<p>Основы криптографии:</p> <ul style="list-style-type: none"> <li>-симметричная и асимметричная криптография;</li> <li>-принципы шифрования, подписи, аутентификации;</li> <li>-наиболее распространенные алгоритмы (RSA, DSA, эллиптические кривые, AES, DES, GQ)</li> </ul> <p>Реализация криптографии:</p> <ul style="list-style-type: none"> <li>-безопасная электронная почта, применение электронных подписей;</li> <li>-управление доступом к ресурсам, сетевая безопасность;</li> <li>-сертификаты, управление ключами, PKI</li> </ul>
<b>Развитие криптографического программного обеспечения</b>	<p>Практическая реализация на языке программирования одной из тем:</p> <ul style="list-style-type: none"> <li>-RSA на практике: генерация простых чисел, эффективной реализации арифметики, деление Montgomery, и т.д ;</li> <li>-Булевы функции и алгебраические атаки;</li> <li>-Реализация криптографических секретных алгоритмов, ключей, хэш-функции и псевдослучайные генераторы;</li> <li>-Реализация криптоанализа</li> </ul>
<b>Смарт-карты и JavaCard</b>	<ul style="list-style-type: none"> <li>-ISO 7816 стандарт совместимости смарт-карт;</li> <li>-Чип реализации ассемблера, стандарт шифрования;</li> <li>-Промышленные приложения, архитектура, спецификация. Кредитные карты, телефоны, платное телевидение;</li> <li>-Атаки на смарт-карты: анализ энергопотребления, машинного времени;</li> <li>-Технология информационной безопасности (Common Criteria ISO 15408);</li> <li>-Java Card 3.0. Приложение смарт-карты.</li> </ul>
<b>Сертификация и безопасное ПО</b>	<p>Целью данного курса является обучение студентов определения ключевых моментов при разработке безопасного программного обеспечения или аппаратных средств.</p> <p>Содержание:</p> <ul style="list-style-type: none"> <li>-Определение и анализ риска (идентификация угроз, предположения на использование продукта, и т.д.);</li> <li>-Методы реализации: разработка методологии оценки доверия (Common Criteria), инструменты для статического анализа кода (борьба с переполнением буфера и других атак), динамических систем защиты.</li> </ul> <p>В конце курса студенты применяя системный подход должны создать безопасный продукт для третьей стороны.</p>
<b>UML и безопасность</b>	<ul style="list-style-type: none"> <li>-Моделирование и спецификация программного обеспечения с использованием универсального языка моделирования;</li> <li>-Моделирование систем безопасности, моделирование атак, моделирование защиты собственности и политик безопасности</li> </ul>

Таблица К.3 – Учебный план программы «Компьютерная безопасность» (магистратура) университета образовательной города Лиможа. Специализированные дисциплины.

Дисциплина	Содержание
<p><b>Криптография и безопасность</b></p> <p><b>Семестр 1</b></p>	<p><b>Цель дисциплины:</b> представить обзор основных алгоритмов шифрования, аутентификации и электронной подписи.</p> <p><b>Содержание дисциплины:</b></p> <ul style="list-style-type: none"> <li>-секретный ключ шифрования, Public Key Cryptography;</li> <li>-Brute атака;</li> <li>-атаки на шифротекст;</li> <li>-интерактивные и неинтерактивные словари для атак;</li> <li>-поточковый шифр, блочный шифр;</li> <li>-транспонирование / замещения модели. Сеть Feistel;</li> <li>-DES, AES;</li> <li>-функции хеширования;</li> <li>-алгоритмы обмена ключами;</li> <li>-RSA алгоритмы с нулевым разглашением;</li> <li>-применение</li> </ul>
<p><b>Основы криптографии</b></p> <p><b>Семестр 3</b></p>	<p><b>Цель дисциплины:</b> дать понятия о симметричных и асимметричных криптосистемах, их безопасности.</p> <p><b>Содержание дисциплины:</b></p> <ul style="list-style-type: none"> <li>-контекст симметричной криптографии: вопросы криптографии, различие между симметричной и асимметричной криптографией;</li> <li>-понятие безопасности: безусловное доказательство;</li> <li>-примеры исторических шифров, основанные на принципах, применяемых в современных алгоритмах (Enigma, Vigenere, Хилл Вернама);</li> <li>-общие понятия алгоритмов блочного шифра;</li> <li>-фейстеля сети: история, описание и свойства DES;</li> <li>-SPN сети: история и описание AES;</li> <li>-режимы работы (ECB, CBC, CFB, OFB);</li> <li>-атаки на криптосистемы (криптоанализ): перебор, линейный и дифференциальный криптоанализ;</li> <li>-мотивация для асимметричной криптографии;</li> <li>-введение в теорию сложности вычислений;</li> <li>-проблема Диффи-Хеллмана (DH);</li> <li>-проблема факторизации. Изучение сложности. Факторизация алгоритмов (Решето Эратосфена, Поллард);</li> <li>-RSA: использование шифрования, RSA-P проблема, связанная с факторизацией ссылки;</li> <li>-задачи дискретного логарифмирования. Изучение сложности (DL). Алгоритм дискретного логарифмирования (расчетный показатель);</li> <li>-Эль Гамаль алгоритм шифрования. Связь с задачей дискретного логарифмирования;</li> <li>-функция сжатия и хэш. Свойства безопасности;</li> <li>-понятие подписи. Определение, RSA, DSA.</li> </ul>
<p><b>Промышленная криптология</b></p> <p><b>Семестр 3</b></p>	<p><b>Цель дисциплины:</b> Дать понятия криптографических протоколов, используемых для безопасности системы обмена информацией.</p> <p><b>Содержание дисциплины:</b></p> <ul style="list-style-type: none"> <li>-хэш-функции и алгоритмы MAC;</li> <li>-подписание протоколов и стандартов;</li> <li>-распределение и обмен ключами;</li> <li>-криптография и эллиптические кривые;</li> <li>-физические атаки;</li> <li>-атаки на дополнительные каналы</li> </ul>

Дисциплина	Содержание
<p><b>Концепции безопасности сетей</b></p> <p>Семестр 3</p>	<p><b>Цель дисциплины:</b> познакомить студентов с принципами безопасности, которые лежат в основе различных систем компьютерной безопасности.</p> <p><b>Содержание дисциплины:</b> -протокол безопасности IPv4/IPv6; -сетевая архитектура (брандмауэр, разбиение на разделы и т.д.); -VPN (IPSec, и т.д.)</p>
<p><b>Системы безопасности</b></p> <p>Семестр 3</p>	<p><b>Содержание дисциплины:</b> -аппаратная архитектура; -Unix System Security; -Windows, системы безопасности; -ошибки потока выполнения (переполнение буфера и т.д.); -изолированные системы (SELinux, виртуализация)</p>
<p><b>Безопасность приложений</b></p> <p>Семестр 3</p>	<p><b>Содержание дисциплины:</b> -Internet Protocol Security (DNS, SMTP, HTTP ит.д.); -Packet Inspection (прокси-сервер); -протоколы аутентификации (Kerberos, RADIUS и т.д.); -PKI / SSL стандарты; -безопасности веб-приложений; -Code Insight</p>
<p><b>Обнаружения вторжений и управления инцидентами</b></p> <p>4 семестр</p>	<p><b>Содержание дисциплины:</b> -обнаружение вторжений (NIDS, HIDS); -управление инцидентами; -формы контроля: Выпускной экзамен</p>
<p><b>Охрана безопасности Windows Web</b></p> <p>4 семестр</p>	<p><b>Цель дисциплины:</b> Дать представление об операционных и административных службах операционных систем семейства Windows NT, организации Windows NT доменов, аутентификации, политики безопасности, файловой системе и реестре. Рассмотреть на сетевом уровне механизмы Active Directory, общих ресурсов, реализацию IPsec и фильтрацию сообщений. Изучить методы обеспечения безопасности: сервер IIS, веб-почта, Internet Explorer.</p> <p><b>Содержание дисциплины:</b> -обзор контекста безопасности веб-приложений; -примеры реализации веб-безопасности; -основные инструменты в области веб-безопасности; -типы уязвимостей; -методология измерения риска; -управление веб-безопасностью; -безопасный код;</p> <p><b>Формы контроля:</b> выпускной экзамен</p>
<p><b>Аппаратная безопасность и правовые аспекты</b></p> <p>4 семестр</p>	<p><b>Цель первой части дисциплины:</b> на основе принципов физики показать безопасность аппаратных средств</p> <p><b>Содержание первой части</b> -архитектура и оценки криптографических продуктов; -TEMPEST проблемы тестирования</p> <p><b>Цель второй части:</b> презентация некоторых юридических аспектов, касающихся политики безопасности на предприятии.</p> <p><b>Содержание второй части:</b> -право на безопасность информационных систем; -уголовное право как средство защиты информационных систем; -правовые аспекты подписи и электронных доказательств; -надзор за использованием и торговлей криптографических продуктов</p>

Дисциплина	Содержание
	<p><b>Формы контроля:</b> Выпускной экзамен</p>
<p><b>Безопасность мобильных радиосистем</b></p> <p><b>4 семестр</b></p>	<p><b>Цель дисциплины:</b> привести описание механизмов и протоколов безопасности, архитектуры безопасности GSM, UMTS и Wi-Fi, в том числе механизмы шифрования, аутентификации субъектов и сообщений, отслеживание коммуникаций и вспомогательных механизмов распределения сеансовых ключей. Привести криптографические алгоритмы реализации.</p> <p><b>Содержание дисциплины:</b></p> <ul style="list-style-type: none"> <li>-защита контента: концепция защиты от копирования, правовые аспекты, основные методы для защиты контента, канал изображения, современные тенденции, стандартизация, системы защиты;</li> <li>-концепция "Broadcast Encryption": отправка зашифрованного сообщение для большого числа пользователей, динамический выбор пользователей, защита от коалиции непривилегированных пользователей, зашифрованная трансляция в реальном времени, применение в промышленных областях (телефония, платное телевидение), защита контента на цифровых носителях (CD, DVD);</li> <li>-системы управления цифровыми правами: система DRM (выражение прав, обеспечения соблюдения прав и защиты контента), реальность стандартизации, решения в сфере мобильного и цифрового кино;</li> <li>-водяные знаки: код, документ, изображение, звук, пример ЦВЗ, стадии интеграции. основные методы реализации психо-визуальной маскировки, области преобразования (DCT, всплески, Фурье), коды коррекции ошибок</li> </ul> <p><b>Формы контроля:</b> выпускной экзамен, демонстрация разработанной концепции защиты контента.</p>



**ПРИЛОЖЕНИЕ К****Аннотация к рабочей программе**

по дисциплине Б1.В.ОД.4 Избранные вопросы информационной безопасности  
Специальность: 10.03.01 Информационная безопасность  
Уровень высшего образования: Бакалавр  
Формы обучения: очная  
Тамбов - 2021

**Автор программы:**

старший преподаватель Анурьева М.С.

Рабочая программа составлена в соответствии с ФГОС ВО.

Рабочая программа рассмотрена и одобрена на заседании выпускающей кафедры ММиИТ  
Протокол №9 от 18.05.2021 года.

1. Цель дисциплины – формирование у студентов целостной картины ранее полученных теоретических знаний и практических навыков по информационной безопасности и компьютерной экспертизы.

2. Содержание курса:

**Тема 1. Лицензирование и сертификация в информационной сфере.**

**Лекция.** Понятия лицензирования и сертификации. Нормативные и правовые документы в области лицензирования и сертификации. Органы лицензирования.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Классификация сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.** Классификация, основные характеристики и особенности использования сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.

**Тема 2. Внутренние нормативные документы по ИБ.**

**Лекция.** Концепция обеспечения информационной безопасности. Политика ИБ. Обязательство о неразглашении защищаемых сведений. Перечень защищаемых сведений. Положение о работе с защищаемыми сведениями.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Стеганографические методы защиты информации, принципы скрытия информации в текстовых документах, в графических изображениях.** Основные особенности, характеристика стенографических методов защиты информации, электронная подпись, методы скрытия информации в текстовых документах, в графических изображениях.

**Тема 3. Система управления информационной безопасностью предприятия.**

**Лекция.** Основные функции систем управления информационной безопасностью. Принципы управления информационной безопасностью. Понятие риска. Идентификация рисков. Оценка вероятности реализации угроз. Оценивание рисков. Измерение рисков. Допустимый уровень риска.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Методы обнаружения и противодействия вредоносным программам.** Обнаружение неизвестного вируса. Основные правила защиты. Восстановление пораженных объектов. Обнаружение троянской программы. Защита от программных закладок и шпионов. Антивирусное программное обеспечение. Обзор современных антивирусных программ. Методика использования антивирусных программ. Прогнозы развития антивирусного обеспечения.

#### **Тема 4. Компьютерные правонарушения.**

**Лекция.** Понятие и виды компьютерных правонарушений. Правовая основа. Методы борьбы.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. Выделите предметы и задачи компьютерной экспертизы.
2. Что такое инцидент информационной безопасности.
3. Проведите анализ законодательной базой регулирования компьютерного преступления.
4. Какое деяние может считаться уголовно наказуемым.
5. Перечислите этапы компьютерной экспертизы.
6. На какие группы классифицируются лица совершившие компьютерные преступления.
7. Перечислите причины инцидента компьютерного преступления.
8. Что является объектами программно-компьютерной экспертизы.
9. На какие группы делятся методы исследования программного обеспечения.

#### **Тема 5. Расследование инцидентов информационной безопасности.**

**Лекция.** Комиссия по расследованию инцидента информационной безопасности. Контекстный поиск информации на диске. Алгоритмы поиска данных. Программное обеспечение по сбору доказательств. Анализ истории и файлов браузера.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. С помощью каких алгоритмов осуществляется поиск данных.
2. Какие файловых менеджеров используются и как они применяются.
3. Какие угрозы могут быть связаны с cookie файлами.
4. Способы получения злоумышленником информации из cookie файлов.
5. Перечислите методы предотвращения возникновения угрозы инцидента информационной безопасности.

#### **Лабораторные задания**

1. Просмотр и клонирование носителей данных
2. Редактор двоичных файлов
3. Сканирование локальной сети

#### **Тема 6. Общая схема расследования цифровых преступлений.**

**Лекция.** Этапы и первоочередные мероприятия при расследовании цифровых преступлений. Специальные методы в компьютерной криминалистике. Корреляция события и анализ временных меток. Инструменты для сохранения целостности цифровых доказательств. Волатильные данные.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. Постройте схему организации взлома защитных механизмов информационных систем.
2. Какими законодательными актами регулируются наказания за неправомерный доступ к охраняемой законом информации.
3. Распишите общую схему расследования преступления.
4. Какие существуют признаки несанкционированного доступа.

5. Как определяется место и время совершения преступления.
6. Опишите последовательность действий расследования, создания и распространения вредоносного ПО.
7. Что может повлиять на сбор волатильных данных?

#### **Лабораторные задания**

1. Анализ времени активности компьютера
2. Анализ локальной сети
3. Восстановление данных
4. Восстановление потерянных разделов

### **Тема 7. Сбор доказательств.**

**Лекция.** Анализ файловых систем и файлов. Сбор доказательств в сетях. Анализ информации проходящей по проводной, радио, оптической и другим электромагнитным системам связи (электросвязи). Вопрос целесообразности и законности хранения информации о действиях пользователя. Сбор доказательств в социальных сетях.

#### **Задания для самостоятельной работы**

1. Как осуществляется поиск доказательств преступлений в файловой системе.
2. На что подразделяются следы в системных областях файловой системы.
3. Какие существуют методы сбора данных о пользователе.
5. Какой закон регулирует законодательный уровень накопления данных в сетях.
6. Какие самые популярные преступления в социальных сетях.

#### **Лабораторные задания**

1. Сбор данных о USB устройствах
2. Блокировка и запрет работы с USB портами

### **Тема 8. Менеджмент информационной безопасности в бизнесе.**

**Лекция.** Информационная составляющая бизнеса. Актуальность вопросов защиты информации в управлении ИТ-инфраструктурой бизнес-компании. Стратегии обеспечения информационной безопасности бизнеса. Моделирование информационных угроз в бизнес-структурах. Инвестиции в информационной безопасности. Управление изменениями в ИКТ-инфраструктуре. Безопасность систем с клиентскими данными.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. На примере организации N оцените надежность используемых методик оценки рисков.
2. Почему необходимо использовать ресурс искусственного интеллекта для анализа угроз ИБ?
3. Как происходит оценка риска компании, согласно методикам, основанным на проверке соответствия обязательным требованиям стандартов и нормативно-правовых

**Лабораторная работа. Тесты на проникновение (пен-тесты).** Место сканеров безопасности в комплексе средств защиты. Задачи локальных и сетевых сканеров безопасности. Объекты сканирования

### **Тема 9. Информационные угрозы бизнеса.**

**Лекция.** Деструктивное программное обеспечение различных модификаций. Массовые и точечные фишинговые атаки на организации. Бизнес-разведка. DDoS-атаки. Таргетированные атаки. Снижение рисков инсайдерских угроз.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. Проанализируйте статистику инцидентов информационной безопасности на предприятии.
2. Какие инциденты приносят наибольший урон предприятию?

**Лабораторная работа. Электронные ключи.** Типизация, внутренняя структура, назначение. Базовые способы и возможности защиты программного обеспечения с помощью электронных ключей. Типовые решения в области организации ключевых систем. Утверждение о подмене эталона

### **Тема 10. Обеспечение информационной безопасности бизнеса.**

**Лекция.** Методика риск-ориентированного подхода к обеспечению доступности, целостности и конфиденциальности данных на современном предприятии. Методика оценки рисков информационной безопасности. Инструменты управления рисками. Защита данных (данных клиента, финансовых данных) от таргетированных атак.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля. документов по оценке и управлению рисками информационной безопасности?

1. По какому алгоритму происходит процесс оценки и управление риском на предприятии?
2. На примере своей организации опишите процесс поэтапного внедрения нейросетей для обнаружения вредоносных атак.
3. На основе циклической оценки и обработки рисков проанализируйте угрозы бизнес-процессам и данным компании N.
4. Оцените ценность активов вашей компании по четырехбалльной система.
5. Используя данные вашей компании, проведите проверку защищенности всей системы от актуальных угроз.
6. Рассчитайте время реакции системы безопасности компании N на произвольный инцидент информационной безопасности.

**Лабораторная работа. Классификация сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.** Классификация, основные характеристики и особенности использования сканеров безопасности: по отношению к объекту сканирования, по назначению, уязвимости.

### **Тема 11. Обеспечение кибербезопасности данных и безопасности ИТ систем в бизнесе**

**Лекция.** Обеспечения кибербезопасности данных и цифровой безопасности промышленных систем. Основные проблемы информационной безопасности ERP-систем, защита систем класса ERP. Применение ERP для обеспечения кибербезопасности промышленных систем и данных.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

1. Дайте определение понятию ERP-система.
2. Из каких уровней состоит типовая ERP-система?
3. Перечислите основные угрозы, характерные для уровня ОС в архитектуре ERP системы.
4. Постройте модель злоумышленника, представляющего наибольшую опасность для ERP-систем.
5. Что необходимо применить для повышения безопасности ERP систем?
6. Выделите основные классификации внутренних угроз и разработайте методы борьбы с ними в ERP- системах.
7. Разработайте комплекс мер по борьбе угрозами на уровне операционной системы.
8. Разработайте методы борьбы с угрозами на уровне архитектуры ERP-системы.
9. Разработайте методы борьбы с угрозами на уровне представлений и приложений.
10. Разработайте методы борьбы с угрозами, характерными уровню СУБД, БД архитектуры ERP-системы.

**Лабораторная работа. Электронная подпись.** Понятие целостности данных и аутентификации источника данных. Задачи защиты информации, решаемые с помощью электронной подписи. Понятие о проверке электронной подписи. Пример реализации ЭП с помощью криптосистемы Эль-Гамала. Понятие о проверке электронной подписи.

**Лабораторная работа. Блокирование информационных угроз для пользователя.** Юридические методы. Организационные меры и основные правила работы за компьютером. Программные методы. WOT. Фильтрация контента. Нормы этического поведения в информационной среде.

### **Тема 12. Модель угроз. Угрозы безопасности информации**

**Лекция.** Понятие уязвимости. Классификация угроз. Стихийные бедствия и пожары; сбои и отказы технических средств. Угрозы утечки информации по техническим каналам. Непреднамеренные и умышленные действия пользователей. Понятие модели нарушителя. Классификация нарушителей: внешние и внутренние нарушители. Предположения об имеющейся у нарушителя информации. Описание каналов атак. Описание объектов и целей атаки. Средства осуществления атак. Способы осуществления атаки.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Асимметричные шифры. Шифр RSA.** Понятие асимметричной системы шифрования. Понятие открытого и секретного ключа. Алгоритм шифрования и расшифрования RSA и его математическое обоснование. Стойкость алгоритма. Рекомендуемые требования к параметрам ключа

### **Тема 13. Стандарты по информационной безопасности**

**Лекция.** Показатели требований к безопасности информации. Практические рекомендации по организации ИБ. Стандарт по информационной безопасности ГОСТ 17799, ГОСТ 27001. Модель и требования для создания, внедрения, эксплуатации, сопровождения и совершенствования системы управления ИБ (СУИБ).

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Асимметричные шифры. Шифр Эль-Гамала.** Понятие асимметричной системы шифрования. Понятие односторонней функции и функции-«ловушки». Алгоритм шифрования и расшифрования Эль-Гамала и его математическое обоснование. Рекомендации по выбору параметров ключа.

### **Тема 14. Системы идентификации и аутентификации**

**Лекция.** Парольные подсистемы идентификации и аутентификации личности. Количественная оценка стойкости парольной защиты. Аппаратные устройства идентификации и аутентификации.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Лабораторная работа. Блочные шифры. Шифр ГОСТ 28147-89.** Парольные подсистемы идентификации и аутентификации личности. Количественная оценка стойкости парольной защиты. Аппаратные устройства идентификации и аутентификации. Режим простой замены, режим шифрования с обратной связью, режим гаммирования с обратной связью, режим гаммирования. Получение ключевой хэш-функции с использованием режима выработки имитовставки.

## 4. Контроль знаний обучающихся

### 4.1 Типовые задания текущего контроля

#### **Типовые темы рефератов.**

- Шифр RSA
- Рекомендуемые требования к параметрам ключа.
- Получение ключевой хэш-функции с использованием режима выработки имитовставки

- Неполадки DHCP
- Задачи локальных и сетевых сканеров безопасности
- Восстановление пораженных объектов.
- Назначение бесключевых хэш-функций.

### Типовые задания блиц-опроса / собеседования

1. Организационные меры и основные правила работы за компьютером.
2. Определение надежности персональных межсетевых экранов
3. Базовые способы и возможности защиты программного обеспечения с помощью электронных ключей
4. Понятие о проверке электронной подписи
5. Преимущества и недостатки систем с симметричными ключами
6. Понятие блочного шифра
7. Дать определение информационной безопасности
8. Дать определение компьютерная экспертиза
9. Дать определение инцидента в сфере информационной безопасности
10. Что является уголовно наказуемым деянием
11. Что такое алгоритм и дать пример алгоритма для поиска данных

### Типовые задания тестирования

1. Что относится к объектам программно-компьютерной экспертизы?
  - a. Операционные системы, утилиты, прикладные программы
  - b. Операционные системы, утилиты, программные средства для разработки программного обеспечения, прикладные программы.**
  - c. программные средства для разработки программного обеспечения, прикладные программы
  - d. Прикладные программы, утилиты
2. Дать определение инцидент информационной безопасности
  - a. Событие, случай, недоразумение, происшествие
  - b. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ.**
  - c. Событие, в котором нарушаются файлы
3. Что относится к угрозам связанные с cookie файлами.
  - a. Утечка конфиденциальной информации, несанкционированный доступ злоумышленника к некоторым web-сервисам от имени пользователя.**
  - b. Кража логинов с помощью клавиатурных вирусов
  - c. Уничтожение файлов на компьютере
4. Что относится к признакам несанкционированного доступа
  - a. Изменение обоев на рабочем столе компьютера
  - b. Изменение комплектующих системного блока
  - c. Появление в компьютере фальшивых данных, частые сбои в процессе работы компьютеров**
5. Какой закон регулирует законодательный уровень накопления данных в сетях
  - a. 149 ФЗ РФ
  - b. 272 УК РФ**
  - c. 152 ФЗ РФ

6. Что относится к преступлениям в социальных сетях

a. Угон машин, кража вещей

**b. Подделка документов, хищение кредитных карт, клевета**

c. Нанесение вреда чужому имуществу

d. Нанесение вреда здоровью

7. Какие объекты способны по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению

a. Холодильники, микроволновой печи, электрочайники

**b. Персональные компьютеры, модемы, принтеры**

c. Клавиатура, компьютерная мышь

d. Домашний телефон

8. На какие группы разделяются объекты следственного действия

a. Нужные и не нужные

b. Рабочие и сломанные

**c. Предмет традиционных преступных посягательств и орудия совершения преступлений**

4.2. Промежуточная аттестация по дисциплине проводится в форме экзамена.

**ПРИЛОЖЕНИЕ Л****Аннотация к рабочей программе**

По дисциплине Б1.Б.5 Основы информационной безопасности  
Направление подготовки 10.03.01 - Информационная безопасность

Уровень высшего образования: Бакалавриат

Формы обучения: очная

Тамбов, 2017

**Автор программы:**

старший преподаватель Анурьева М.С.

Рабочая программа составлена в соответствии с ФГОС ВО.

Рабочая программа принята на заседании кафедры ММиИТ «03» июня 2017 года  
Протокол №6.

**1. Цели и задачи дисциплины**

1.1 Цель дисциплины – изучение основных общеметодологических основ информационной безопасности.

В рамках изучения дисциплины предусматривается прохождение вендорского курса Сетевой академии Cisco «Введение в кибербезопасность» (Introduction to Cybersecurity). Курс представляет собой набор теоретического материалы, практических и лабораторных работ, заданий для самоконтроля. Контроль по темам осуществляются путем тестирования. Завершается изучение курса прохождением итогового тестирования, при успешной сдаче которого студент получает сертификат о прохождении курса.

**2. Место дисциплины в структуре ОП бакалавриата:**

Дисциплина «Основы информационной безопасности» относится к дисциплинам базовой части учебного плана ОП ВО.

Дисциплина изучается во 2 семестре.

**3. Объем и содержание дисциплины**

3.2. Содержание курса:

**Тема 1. Нормативно-правовые основы информационной безопасности.**

**Лекция.** Структура. Основные законы. Нормы и регламенты регулирующих органов. Нормативное регулирование вопросов обеспечения информационной безопасности в регионе и в конкретной организации. Отечественные и зарубежные стандарты.

**Задания для самостоятельной работы.**

1. Изучить федеральное законодательство РФ по вопросам защиты информации.
2. Изучить стратегические национальные документы.

**Лабораторная работа.** Изучение Доктрины ИБ РФ.



## **Тема 2. Информационная безопасность государства.**

**Лекция.** Структура органов власти, обеспечивающих безопасность в информационной сфере. Регуляторы в сфере ИБ, сфера компетенций в области защиты информации.

**Задания для самостоятельной работы.**

Изучение теоретического материала Главы 0 «Знакомство с курсом» и Главы 1 «Потребность в кибербезопасности» курса «Введение в кибербезопасность» Сетевой академии Cisco.

**Лабораторная работа.** Лабораторная работа по программно-аппаратным методам защиты информации из курса Сетевой академии Cisco «Введение в кибербезопасность».

## **Тема 3. Терминологические основы информационной безопасности. Основные понятия и определения.**

**Лекция.** Защита информации, информационная безопасность, тайна, средства защиты информации. Угрозы и уязвимости. Конфиденциальность, целостность, доступность.

**Задания для самостоятельной работы.** Повторение пройденного материала по курсу Сетевой академии Cisco «Введение в кибербезопасность».

**Лабораторная работа.** Анализ терминов и определений информационной безопасности.

## **Тема 4. Теоретический базис защиты информации**

**Лекция.** Особенности научно-методологического базиса решения задач защиты информации. Методологический базис теории защиты информации.

**Задания для самостоятельной работы.**

Изучение теоретического материала Главы 2 «Атаки, понятия и техники» курса «Введение в кибербезопасность» Сетевой академии Cisco.

**Лабораторная работа.**

1. Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации.

2. Лабораторная работа по программно-аппаратным методам защиты информации из курса Сетевой академии Cisco «Введение в кибербезопасность».

## **Тема 5. Принципы теории информационной безопасности.**

**Лекция.** Этапы развития информационной безопасности. Требования к системе ЗИ. Показатели информации.

**Задания для самостоятельной работы.** Повторение пройденного материала по курсу Сетевой академии Cisco «Введение в кибербезопасность».

**Лабораторная работа.** Лабораторная работа по программно-аппаратным методам защиты информации.

## **Тема 6. Безопасность в киберпространстве**

**Лекция.** Разграничение понятий информационная и компьютерная безопасность. Защита информации в киберпространстве. Атаки и уязвимости в виртуальном мире. Средства и методы защиты. Государственное регулирование. Приоритеты для обеспечения безопасности киберпространства

**Задания для самостоятельной работы.**

Изучение теоретического материала Главы 3 «Защита данных и конфиденциальности» курса «Введение в кибербезопасность» Сетевой академии Cisco.

**Лабораторная работа.** Лабораторная работа по программно-аппаратным методам защиты информации из курса Сетевой академии Cisco «Введение в кибербезопасность».

### Тема 7. Угрозы информационной безопасности.

**Лекция.** Понятие и виды. Характер и источники угроз. Предпосылки появления угроз.

**Задания для самостоятельной работы.**

Изучение теоретического материала Главы 4 «Защита организации» курса «Введение в кибербезопасность» Сетевой академии Cisco.

**Лабораторная работа.** Лабораторная работа по программно-аппаратным методам защиты информации из курса Сетевой академии Cisco «Введение в кибербезопасность».

### Тема 8. Методы нарушения конфиденциальности, целостности и доступности информации.

**Лекция.** Стратегии защиты информации. Архитектура систем защиты информации. Семирубежная модель защиты информации.

**Задания для самостоятельной работы.** Повторение пройденного материала по курсу Сетевой академии Cisco «Введение в кибербезопасность».

**Лабораторная работа.**

1. Лабораторная работа по программно-аппаратным методам защиты информации.
2. Прохождение итогового тестирования по курсу Сетевой академии Cisco «Введение в кибербезопасность».

### Тема 9. Утечка информации.

**Лекция.** Понятие утечки информации. Основные виды утечки информации (умышленные, случайные, внешние, внутренние). Каналы утечек информации (технические, материально-вещественные, акустические и проч.). Введение в способы защиты от утечек информации.

**Задания для самостоятельной работы.** Повторение пройденного материала по курсу Сетевой академии Cisco «Введение в кибербезопасность».

**Лабораторная работа.** Изучение средства радиотехнического контроля «Скорпион»

### Тема 10. Информационная безопасность региона

**Лекция.** Понятие. Структура. Компоненты. Политики ИБ в отдельных организациях.

**Задания для самостоятельной работы.** Повторение пройденного материала по курсу Сетевой академии Cisco «Введение в кибербезопасность». Итоговое тестирование. Отзыв по курсу.

**Лабораторная работа.** Оценка безопасности информации на объектах ее обработки.

#### 4. Типовые задания текущего контроля

##### Типовые темы рефератов.

1. Модель нарушителя информационной безопасности
2. Повышение надежности информационной системы.
3. Защита информации от инсайдерских угроз
4. Наиболее распространенные угрозы доступности, целостности и конфиденциальности.


4.4. Промежуточная аттестация по дисциплине проводится в форме экзамена.

**Типовые вопросы экзамена**

1. Составляющие информационной безопасности
2. Защита данных и конфиденциальности.
3. Атаки, понятия и техники
4. Обеспечение безопасности в киберпространстве
5. Структура законодательства РФ
6. Характер и источники угроз. Предпосылки появления угроз
7. Архитектура систем защиты информации
8. Классификация угроз информационной безопасности (угрозы целостности, конфиденциальности и доступности)
9. Угрозы информационной безопасности: по природе возникновения, по степени преднамеренности проявления, по непосредственному источнику угроз

## ПРИЛОЖЕНИЕ М

Пример студенческого сертификата учебного курса с начального уровня «Введение в кибербезопасность» Сетевой академии Cisco



**Сертификат о прохождении курса**

Подтверждает:

**Lina Kalashnikova**

прохождение курса Cisco Networking Academy® «Введение в Кибербезопасность» и обладание следующими навыками и знаниями.

- Понятия и важность кибербезопасности
- Характеристики и последствия разных типов кибератак
- Как защитить себя от кибератак
- Техники, используемые для защиты организаций от кибератак
- Почему профессия специалиста по информационной безопасности становится все более востребованной
- Возможности, доступные для получения сертификации в области сетевой безопасности

**Alexey Samokhvalov**      **Apr 25, 2018**  
 Инструктор      Дата  
*Alexey Samokhvalov*  
 Инструктор

**ПРИЛОЖЕНИЕ Н****Аннотация к рабочей программе**

По дисциплине Б1.Б.14 Системы защиты информации в мире  
Направление подготовки 10.03.01 - Информационная безопасность  
Уровень высшего образования: Бакалавриат  
Формы обучения: очная  
Тамбов, 2017

**Автор программы:**

Старший преподаватель Анурьева М.С.

Рабочая программа составлена в соответствии с ФГОС ВО.

Рабочая программа принята на заседании кафедры ММиИТ «03» июня 2017 года  
Протокол №6.

1 Цель дисциплины – формирование у студентов базовых знаний о государственных системах обеспечения безопасности в информационной сфере, международном сотрудничестве в вопросах защиты информации; формирование навыков поиска и анализа зарубежных источников, в том числе зарубежных баз научных статей, по актуальным проблемам информационной безопасности в мире

В рамках изучения дисциплины в 7 семестре предусматривается прохождение вендорского курса Сетевой академии Cisco «Основы кибербезопасности». В рамках курса рассматриваются вопросы киберпреступности и кибербезопасности, принципы конфиденциальности, целостности и доступности; тактика, методы и процедуры, используемые киберпреступниками; технологии, продукты и процедуры используемые для защиты информации. Курс представляет собой набор теоретического материала, практических и лабораторных работ, заданий для самоконтроля. Контроль по темам осуществляются путем тестирования. Завершается изучение курса прохождением итогового тестирования, при успешной сдаче которого студент получает сертификат международного уровня о прохождении курса.

**2. Место дисциплины в структуре ОП бакалавриата:**

Дисциплина относится к дисциплинам базовой части учебного плана ОП ВО, изучается во 5-7 семестрах.

**3. Объем и содержание дисциплины**

3.1. Объем дисциплины: 17 з.е.

3.2. Содержание курса:

**5 семестр****Тема 1. Обеспечение безопасности в информационной сфере до XX века.**

**Лекция.** Формирование первых органов государственной власти с компетенциями по обеспечению безопасности в информационной сфере и их трансформация.

Государственные взгляды на безопасность информационной сферы в разное время. Информационное противоборство. Информация как средство противостояний.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. В чем заключались функции разрядного приказа как органа, обеспечивающего информационную безопасность государства в 16-17 веках?
2. Опишите основные правовые акты в области защиты информационной сферы в 18 веке.
3. В чем заключались задачи государственных органов в системе защиты информационной сферы в Российской империи 18 века?
4. Какие учреждения осуществляли функции по защите информационной сферы в 19 веке?
5. Как было организовано секретное делопроизводство в военном министерстве в 19 веке?
6. Что относилось к защищаемым сведениям в области коммерческой тайны в 19 веке?

**Практическая работа.** Особенности организации органов по защите информации.

## **Тема 2. Защита информации России в 1900-1917гг.**

**Лекция.** Введение. Защита военной тайны. Организация контрразведывательной службы. Органы по защите военной тайны. Военная цензура печатных изданий. Организация фельдьегерской связи.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. По каким направлениям велась работа по защите военной тайны в начале 20 века?
2. В какой момент были предприняты меры по коренному улучшению организации контрразведывательной службы и почему (начало 20 века)?
3. Опишите уровень шифростойкости отечественных шифров в начале 20 века. Представляли ли они трудности для криптоаналитиков того времени? Почему?

**Практическая работа.** Влияние деятельности иностранных служб на отдельные события в России.

## **Тема 3. Обеспечение национальной безопасности в информационной сфере в первой половине XX века**

**Лекция.** Система защиты информационной сферы СССР до начала ВОВ.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. С какой целью была основана ВЧК?
2. Почему ВЧК была реформирована в ГПУ?
3. Какие задачи выполняла ВЧК?
4. Кем был смещен Ф.Э. Дзержинский и в связи с чем?
5. Были ли у ВЧК особые полномочия, если да, то какие?
6. С какими событиями связан переход ГПУ к ОГПУ?

**Практическая работа.** Информационная война в начале 40х XX века

## **Тема 4. Информационная безопасности и защита информации в период Великой Отечественной Войны.**

**Лекция.** Народный комиссариат внутренних дел СССР. Состав. Независимые контрразведывательные организации СМЕРШ. Органы разведки в период ВОВ. Криптографические и технические методы защиты информации в военный период. Шифровальная аппаратура.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. В связи с чем и в какой степени применение шифратора «Соболь-П» повлияло на исход боя на Курской дуге?
2. В каких сражениях прошла боевую проверку шифровальная машина М-100?
3. Что было общего у шифровальных устройств «Сова» и «Нева»?
4. Охарактеризуйте уровень развития шифровальной службы СССР к концу войны.

**Практическая работа.** Криптографическая защита данных.

### **Тема 5. Система безопасности СССР во второй половине 40-х – первой половине 50-х гг. XX века.**

**Лекция.** Последствия войны и новые тенденции в развитии общества. Система двублокового противостояния в мире. Три этапа становления государственной безопасности СССР. Внешняя разведка. Военная разведка.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. В чем состоит главная причина неудач политики коллективной безопасности в послевоенный период?
3. Основные задачи органов «Смерш»–НКГБ–МГБ непосредственно после завершения войны?
4. Какая задача была поставлена Правительством СССР перед внешней разведкой в первой половине 50х годов?
5. Чем занимались два управления Министерства госбезопасности (ПГУ МГБ)?
6. Что стало важнейшим явлением послевоенного периода истории правительственной связи и криптографии?

**Практическая работа.** Организация защиты информации в послевоенный период.

### **Тема 6. Организация защиты государственных секретов и система безопасности во второй половине 50-90 гг.**

**Лекция.** Министерство Государственной Безопасности СССР. Структура МГБ. Причины реорганизаций. Комитет государственной безопасности СССР. Структура КГБ СССР. Основные задачи КГБ.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. В чем заключалось отличие практики МГБ от предшествующих ей структур (НКВД, ВЧК)?
2. С какой целью было создано Центральное бюро по рационализации и изобретательству?
3. Что входило в обязанности 1-го отдела 1-го главного управления МГБ?
4. Опишите основные исторические этапы развития КГБ.

**Практическая работа.** Изучение актуальных отечественных алгоритмов криптографической защиты информации.

### **Тема 7. Современная система защиты информации в РФ.**

**Лекция.** Органы обеспечения национальных интересов в информационной сфере России в современное время.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Перечислите основные направления деятельности ФСБ.
2. В каких сферах деятельности ФСБ активно сотрудничает с другими спецслужбами?
3. Опишите структуру органов государственной охраны
4. Опишите, в чем заключается деятельность ФСО в сфере защиты информации.
5. В чем состоит деятельность Ученого совета в работе Совета Безопасности РФ?
6. Какими особыми правами наделяется Государственная фельдъегерская служба для выполнения возложенных на нее задач?
7. Кто может являться владельцем отправлений особой важности, совершенно секретных, секретных и иных служебных отправлений, доставку которых обеспечивает ГФС РФ?
8. Кто осуществляет координацию и руководство деятельностью Службы специальных объектов при Президенте РФ?
9. Каковы полномочия Службы внешней разведки?
10. Какие функции выполняет ФСТЭК?
11. Кто осуществляет руководство деятельностью ФСТЭК?

**Практическая работа.** Государственных органов, регулирующие вопросы защиты информации

### **Тема 8. Проблемы обеспечения информационной безопасности в России.**

**Лекция.** Что такое информационная безопасность: различные подходы к определению. Исторические предпосылки. Регуляторы в области информационной безопасности. Система сертификации по требованиям безопасности.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Охарактеризуйте сферу интересов в информационной безопасности для различных категорий должностей организации.
2. Что включает в себя "информационная сфера"?
3. Какие исторические предпосылки способствовали формированию современной системы защиты информации в России?
4. Перечислите сферу компетенций различных регуляторов в области информационной безопасности. В чем их компетенции пересекаются?
5. В чем отличие отечественной системы сертификации от международной?

**Практическая работа.** Изучение системы отечественных стандартов информационной безопасности.

### **Тема 9. Лицензирование в области защиты информации и сертификация средств защиты информации.**

**Лекция.** Лицензирование. Аттестация объектов информатизации. Сертификация. Классификация средств защиты. Деятельность органов-регуляторов в сертификации и лицензировании в области защиты информации. Реестр сертифицированных средств.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Что составляет организационную структуру системы государственного лицензирования?
2. Охарактеризуйте сферу компетенций органов, уполномоченных на ведение лицензионной деятельности.
3. Какие виды деятельности по защите информации подлежат лицензированию?
4. Что может послужить основанием для отказа в выдаче лицензии?
5. Чем лицензирование отличается от сертификации?
6. Что такое класс безопасности? Какие классы вы знаете?

**Практическая работа.** Изучение актуальных средств технической защиты информации.

### **Тема 10. Обеспечение информационной безопасности при борьбе с терроризмом.**

#### **Кибертерроризм.**

**Лекция.** Терминологическая база: терроризм, террорист, террористическая группа, террористическая организация, террористическая деятельность. Международная террористическая деятельность. Принципы борьбы с терроризмом. Структурная схема взаимодействия субъектов, осуществляющих борьбу с терроризмом. Федеральная антитеррористическая комиссия. Кибертерроризм: понятие и примеры реализации.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Чем террористическая группа отличается от террористической организации?
2. Что относят к террористической деятельности?
3. Какие органы государственной власти занимаются борьбой с терроризмом? Охарактеризуйте их компетенции в данной сфере.
4. Какие права имеют лица, в зоне проведения контртеррористической операции, проводящие эту операцию?

**Практическая работа.** Типы информационного оружия: история и современность.



## 6 семестр

**Тема 11. Формирование взглядов на обеспечение информационной безопасности в зарубежных странах.**

**Лекция.** Защита информации в древности (Древние Германия, Древние Греция и Рим, Древние Египет и Месопотамия, Страны Ближнего Востока, Древняя Индия, Древняя Япония, Древний Китай). Защита информации в средние века (Средневековая Европа). Защита информации в 17-19 веках. Защита информации в 1-й половине XX в. Защита информации во время второй мировой войны. Защита информации во второй половине XX в.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Практическая работа.** Криптографическая защита информации на начальном этапе.

**Тема 12. Состояние проблемы информационной безопасности в странах Евросоюза.**

**Лекция.** Европейское агентство по сетевой и информационной безопасности (ENISA) и государственные стратегии кибербезопасности. Центр по борьбе с киберпреступностью. Ближайшие проекты Евросоюза.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Что такое информационное оружие?
2. Какова основная особенность информационного оружия?
3. С какой целью было создано Европейское агентство по сетевой и информационной безопасности?
4. Какие факторы оказывают влияние на функционирование ключевых информационных систем общего пользования?
5. Что такое кибербезопасность?
6. Для чего ENISA разработало специальное руководство Good Practice Guide on NCSS?
7. Каковы сферы ответственности Европейского центра по борьбе с киберпреступностью?

**Практическая работа.** Принципы шифрования.

**Тема 13. Система защиты информации в США.**

**Лекция.** История развития взглядов США на понятие «информационная война». Деятельность американской администрации на обеспечение безопасности в информационной сфере. Разведывательное управление (DI). Оперативное управление (DO). Научно-техническое управление (DS&T). Административное управление (DA).

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Перечислите нормативно-правовые акты, регламентирующие государственную политику США в области информатизации.
2. Какую политику должны вести США для успешной реализации положений Концепции национальной безопасности США?
3. Что является результатом реализации положений Концепции национальной безопасности США?
4. Какими директивами Президента США регламентируется решение важные стратегические вопросы национальной политики в сфере информационной безопасности?
5. Что такое «Разведывательное Сообщество» США и какие организации в него входят?
6. Какие органы исполнительной власти США занимаются исключительно разведывательной деятельностью?
7. Какие структурные подразделения входят в состав ЦРУ?
8. Назовите причины и цели создания Министерства внутренней безопасности США.

9. Какие управления и отделы входят в состав Национального управления военно-космической разведки США?

10. Какие методы использует АНБ в своей профессиональной деятельности?

**Практическая работа.** Регуляторы в сфере защиты информации в США

#### **Тема 14. Система защиты информации в Великобритании.**

**Лекция.** Спецслужбы Великобритании. Стандарты ИБ. Структура затрат на защиту информации в правительстве Британии. Программные средства ИБ.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Практическая работа.** Регуляторы в сфере защиты информации в Великобритании.

#### **Тема 15. Государственная система обеспечения информационной безопасности во Франции.**

**Лекция.** Спецслужбы Французской республики. Структура спецслужб Французской республики. ДГСЕ. Управление военной разведки (ДРМ). Структура ДРМ.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Как правительство Франции рассматривает концепцию информационной войны?
2. Чем французское представление экономического конфликта отличается от других европейских стран?
3. В чем преимущество виртуальной войны?
4. Какие методы по мнению французских экспертов обеспечивает надежную защиту информации и какие меры необходимы для достижения этих методов?
5. Что препятствует защитным действиям по предотвращению и снижению угроз информационной войны?

**Практическая работа.** Регуляторы в сфере защиты информации во Франции.

#### **Тема 16. Системы защиты информации в Китае.**

**Лекция.** Организационная структура спецслужб Китая. «Великая стена» информационной безопасности Китая. Министерство государственной безопасности КНР.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля.

**Практическая работа.** . Регуляторы в сфере защиты информации в Китае.

#### **Тема 17. Цифровой суверенитет.**

**Лекция.** Эпоха слома суверенитета. Электронный суверенитет. Кибервойна. Информационный суверенитет. Разработка независимого интернет-доступа.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Что включает в себя «электронный щит» государства?
2. Обладает ли Россия в настоящее время «электронным щитом»?
3. Что включает в себя «информационный щит» государства?
4. Обладает ли Россия в настоящее время «информационным щитом»?
5. Какая страна в наибольшей степени обладает «электронным» и «информационным»

**Практическая работа.** Анализ цифрового суверенитета разных стран.

#### **Тема 18. Международное сотрудничество по информационной безопасности.**

**Лекция.** Итоги работы ООН по вопросам информационной безопасности. Документы, регламентирующие международную информационную безопасность.

**Задания для самостоятельной работы.** Ответить на вопросы для самоконтроля:

1. Перечислите основные международные мероприятия по вопросам информационной безопасности.
2. Какие принципы зафиксированы в Бухарестской декларации?

3. Сформулируйте основные принципы обеспечения международной информационной безопасности.

**Практическая работа.** Особенности защиты персональных данных в ведущих зарубежных странах.

### Семестр 7

#### Тема 20. Кибербезопасность – мир экспертов и преступников.

**Лекция.** Мир кибербезопасности. Домены кибербезопасности. Кибербезопасность: злоумышленники и специалисты. Общие угрозы. Угрозы интернет-услугам. Угрозы ключевым отраслям промышленности. Распространение угроз кибербезопасности: пути распространения и уровень сложности угроз. Дополнительная поддержка безопасности: интернет-сообщества и международная сертификация (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение кибермошенничества.

Кибербезопасность.

Идентификация угрозы.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение специализации по информационной безопасности NISP/NICE.

#### Тема 21. «Куб» кибербезопасности.

**Лекция.** Три измерения куба кибербезопасности: целостность (принцип целостности данных, потребности в целостности, проверка целостности), конфиденциальность (принцип конфиденциальности, защита конфиденциальных данных, управление доступов, международное законодательство) и доступность (принцип доступности, обеспечение доступности). Данные и обеспечение безопасности: типы хранилищ данных, методы передачи данных, проблемы защиты хранимых данных In-Transit, формы обработки и вычисления данных, определение состояния данных. Контрмеры по кибербезопасности. Технологии: программные гарантии безопасности, аппаратные средства защиты, сетевые технологии, облачные технологии. Создание культуры осведомленности о кибербезопасности. Политики и процедуры кибербезопасности: стандарты, методические рекомендации, процедуры. Определение категории противодействия. Система управления ИТ: модель кибербезопасности ISO (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение принципов ИБ.

Определение состояния данных.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Установка виртуальной машины на ПК.

Изучение аутентификации, авторизации и учета.

Изучение шифрования файлов и данных.

Проверка целостности файлов и данных.

#### Тема 22. Угрозы кибербезопасности, уязвимости и атаки.

**Лекция.** Вредоносные программы и вредоносный код. Типы вредоносных программ: вирусы, черви, троянские кони, логические бомбы, вымогатели, бэквоты и руткиты.

Защита от вредоносных программ. Атаки электронной почты и браузера: спам, spyware, adware, scareware, фишинг. Плагины браузера. Защита от атак электронной почты и браузера. Мошенничество: дайвинг, пиггирование и другие методы. Защита от мошенничества. Кибератаки: типы кибератак (отказ в обслуживании, подделки, "человек посередине", атаки с нулевым дном, ведение журнала клавиатуры). Защита от атак. Обнаружение угроз и уязвимости. Атаки и защита беспроводных и мобильных устройств. Настройка WEP/WPA2 Psk/ WPA2 RADIUS. Прикладные атаки: межсайтовый скриптинг, ввод кода, переполнение буфера, удаленное исполнение кода, элементы управления ActiveX и Java. Защита от атак приложений (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение типов вредоносного кода.

Определение атак электронной почты и браузера.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение проблем социальной инженерии.

Определение кибер-атак.

Определение типов приложений и атак.

### **Тема 23. Криптографические методы защиты информации.**

**Лекция.** История криптографии. Создание зашифрованного текста. Изучение шифра Виженера. Два типа шифрования: шифрование с закрытым ключом (процесс симметричного шифрования, типы, алгоритмы), шифрование с открытым ключом (ассиметричный процесс шифрования, алгоритмы). Ключевой менеджмент. Сравнение типов шифрования. Контроль доступа: типы контроля, стратегии, идентификация, методы проверки подлинности, авторизация, подотчетность, типы средства контроля безопасности. Скрытие данные: маскирование, стеганография, обфускация (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Использование симметричного шифрования.

Использование ассиметричного шифрования.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Сравнение симметричного и ассиметричного шифрования.

Определение стратегий контроля доступа.

Определение методов проверки подлинности.

Сравнение типов элементов управления безопасностью.

### **Тема 24. Обеспечение целостности данных.**

**Лекция.** Обеспечение целостности данных. Типы элементов управления целостностью. Цифровые подписи, сравнение алгоритмов цифровой подписи. Использование цифровых подписей. Сертификаты: создание цифрового сертификата, процесс проверки, путь сертификата. Обеспечение соблюдения целостности базы данных: проверка и требования к целостности БД (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение терминологии.

Cracking (взлом) паролей.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Использование цифровых подписей.

Работа с цифровыми сертификатами.

Организация удаленного доступа.

#### **Тема 25. Концепция «пяти девяток».**

**Лекция.** Что такое «пять девяток». Среды, требующие «пять девяток». Угрозу доступности. Проектирование системы высокой доступностью. Меры по улучшению доступности. Управление активами: идентификация активов, классификация активов, стандартизация активов, идентификация угроз, анализ риска. Избыточность. Системная устойчивость. Расследование инцидентов: фазы реагирования на инцидент (подготовка, обнаружение, анализ, восстановление). Технологии реагирования на инцидент: контроль доступа в сеть, системы обнаружения вторжений, системы предотвращения вторжений. аварийное восстановление: планирование восстановлений после стихийных бедствий, планирование непрерывности бизнеса (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Проведение анализа риска активов.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Определение уровня защиты.

Анализ фаз реагирования на инцидент.

#### **Тема 26. Защита домена кибербезопасности.**

**Лекция.** Защитные системы и устройства: укрепление (безопасность ОС, управление патчами, брандмауэры, безопасная связь). Безопасность беспроводных и мобильных устройств: WEP, WPA/WPA2, взаимная аутентификация. Защита данных хоста: контроль доступа к файлам, шифрование файлов, резервное копирование системы и данных. Управление изображениями и контентом: скрининг и блокировка контен. Физическая защита рабочих станций. Безопасность серверов: безопасный удаленный доступ, административные меры, физическая защита серверов. Безопасность сети: защита сетевых устройств, голосовое и видеоборудование. Физическая охрана: контроль доступа и видеонаблюдение (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Безопасность системы Linux.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Защитные системы и устройства.

Серверные брандмауэры и маршрутизаторы ACL.

#### **Тема 27. Специалисты по кибербезопасности.**

**Лекция.** Домены кибербезопасности: пользовательский домен (общие угрозы пользователей и уязвимости, управление угрозами пользователей), домен устройства (общие угрозы устройства, управление угрозами устройства), домен локальной сети (общие угрозы и управление угрозами), частный облачный домен (общие угрозы и управление угрозами), общественный облачный домен (общие угрозы и управление угрозами), домен для физических лиц (общие угрозы и управление угрозами), домен

приложений (общие угрозы и управление угрозами).. Этика работы в ИБ: руководящие принципы, законы и ответственность, информационные сайты) (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

**Задания для самостоятельной работы** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Соответствующие области кибербезопасности.

**Практическая работа** (по материалам курса Сетевой академии Cisco «Основы кибербезопасности»).

Использование соответствующего инструментаЗИ.

Интеграция навыков.

#### 4. Типовые задания текущего контроля

##### Типовые темы рефератов.

1. Анализ фундаментальных процессов, связанных с ведением войны в информационном обществе.
2. Анализ российских юридических норм в области компьютерной экспертизы.
3. Страховая защита информации в системе информационной безопасности.
4. Легальная разведка и сбор информации: традиционные и новейшие методы.
5. Сравнительный анализ сервисов информационной безопасности для пользователя.
6. Появление и развитие правовых средств защиты информации в зарубежных странах.
7. Системы защиты информации в ведущих мировых компаниях (на примере одной компании).

##### Типовые задания блиц-опроса / тестирования

1. Укажите операционную систему, наиболее часто подвергающуюся вирусным атакам.

- a. **Windows**
- b. Unix
- c. Linux

1. В соответствии с Указом Президента России Гостехкомиссия в настоящее время именуется ...

- a. ФСБ
- b. **ФСТЭК**
- c. СВР
- d. ФАПСИ

3. Что НЕ входит в «электронный щит» для обеспечения цифрового суверенитета

- a. **собственная или контролируемая программная платформа**
- b. собственная или контролируемая мобильная платформа
- c. собственная аппаратная платформа
- d. нет верного ответа

4. Кто изобрел машину с вращательными шифровальными дисками с различным количеством букв?



- a. Ж.-Ф.Шампольон
- b. Д. Вадсворт
- c. **А.Тьюринг**
- d. Ч.Уитстон

5. К какому времени относят появление первых специализированных антивирусных программ?

- a. начало 80-х гг
- b. вторая половина 80-х гг
- c. начало 90-х гг**
- d. вторая половина 70-х гг

## ПРИЛОЖЕНИЕ П

**Пример студенческого сертификата учебного курса среднего уровня «Основы кибербезопасности» Сетевой академии Cisco**

 Социальная ответственность компании	Сетевая академия Cisco
Свидетельство об окончании курса	
<b>Cybersecurity Essentials</b>	
Студент успешно прошел курс Cybersecurity Essentials под руководством нижеподписавшегося инструктора. Студент продемонстрировал следующие умения.	
<ul style="list-style-type: none"> <li>• Описать тактику, методы и процедуры, используемые киберпреступниками.</li> <li>• Объяснить, как принципы конфиденциальности, целостности и доступности соотносятся с состояниями данных и средствами противодействия угрозам безопасности.</li> <li>• Объяснить цель законов, относящихся к кибербезопасности.</li> </ul>	<ul style="list-style-type: none"> <li>• Описать технологии, продукты и процедуры, используемые для обеспечения конфиденциальности, целостности и высокой доступности.</li> <li>• Объяснить, как специалисты по кибербезопасности используют технологии, процессы и процедуры для защиты всех компонентов сетевой инфраструктуры.</li> </ul>
<b>Andrey Akashev</b> <small>Учащийся</small>	
<b>Tambov State University</b> <small>Название академии</small>	
<b>Russia</b> <small>Местоположение</small>	
<b>Alexey Samokhvalov</b> <small>Инструктор</small>	
<b>25.10.2018</b> <small>Дата</small>	
 <small>Подпись инструктора</small>	



**ПРИЛОЖЕНИЕ Р****Тест на определение начального уровня теоретической подготовки**

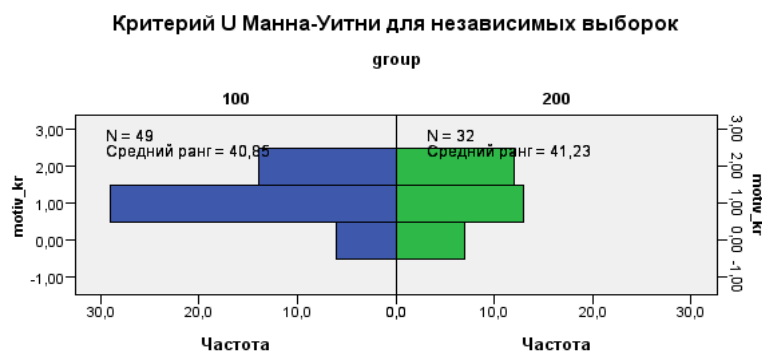
1. Что такое угроза информационной безопасности?
  - a) Возможные события, способные нанести ущерб
  - b) Действия нарушителя по нанесению ущерба субъектам или объектам информации.
  - c) Попытки злоумышленника косвенно изучить архитектуру компьютерной системы
2. Основная цель защиты компьютерных систем:
  - a) Противодействие угрозам безопасности на предприятии
  - b) Принципы разграничения доступа предприятия
  - c) Методы защиты, средства, используемые предприятием
  - d) Скрытие механизмов системы защиты информации
3. Перечислите угрозы безопасности:
  - a) Естественные
  - b) Искусственные
  - c) Социальные
  - d) Экономические
4. Перечислите меры защиты информации компьютерных систем:
  - a) Законодательные
  - b) Административные
  - c) Физические
  - d) Математические
  - e) Организационные
5. Что используют для защиты авторских прав на изображения, фотографии и т.д.
  - a) Заголовки
  - b) Микроточки
  - c) Цифровые водяные знаки
  - d) Симпатические чернила
  - e) Типографские точки
6. К требованиям стеганографии относят:
  - a) В качестве носителя скрытой информации должен выступать объект, допускающий искажения собственной информации, которые нарушают его функциональность и суть
  - b) Размер контейнера должен в несколько раз превышать размер инкапсулируемых данных
  - c) Объект, выступающий в виде носителя скрытой информации, допускающий искажения собственной информации, при этом не нарушающие его функциональность и суть.
  - d) Методы скрытия должны обеспечивать аутентичность и целостность файла
  - e) Размер контейнера должен быть равен размеру инкапсулируемых данных
7. Метод LSB в стеганографии заключается:
  - a) В преобразовании графического изображения.
  - b) В использовании погрешности дискретизации.
  - c) В использовании зарезервированных полей форматов данных.
  - d) В использовании спецификации форматов данных.
  - e) В использовании уменьшенных изображений.
8. Отнесение сведения к государственной тайне осуществляется мотивированным решением государственного эксперта по вопросам тайны. В его решении указывается:

- a) Информация, составляющая государственную тайну
  - b) Обоснования ущерба за разглашение
  - c) Сведения о ЧП
  - d) Степень секретности
  - e) Гриф секретности
9. Основанием для рассекречивания являются:
- a) Принятие на себя РФ международных требований
  - b) Изменение объективных обстоятельств
  - c) Изменение пароля (ключа)
  - d) Изменение способов кодирования
10. Адаптированный к российским критериям стандарт безопасности:
- a) OrangeBook
  - b) ISO/IEK 27001
  - c) ISO/IEK 17799
  - d) ISO 27k
11. К преднамеренным искусственным угрозам относятся:
- a) Физическое разрушение систем
  - b) Хищение носителей информации
  - c) Неумышленная порча носителя информации
  - d) Вход в систему в обход стандартных процедур
12. Источники угроз по отношению к КС могут быть
- a) внешними
  - b) внутренними
  - c) неопределенными
  - d) запланированными
13. Непреднамеренные искусственные угрозы компьютерным системам
- a) неправомерное отключение оборудования
  - b) заражение компьютера вирусами
  - c) несанкционированное использование терминалов пользователей
  - d) игнорирование организационных ограничений
14. К преднамеренным искусственным угрозам можно отнести:
- a) ввод ошибочных данных;
  - b) хищение носителей информации
  - c) физическое разрушение системы
  - d) действия по дезорганизации функционирования системы
15. Основные возможные типы умышленных угроз
- a) незаконное получение паролей и других реквизитов разграничения доступа
  - b) вскрытие шифров криптозащиты информации
  - c) внедрение вредоносных программ
  - d) незаконное подключение к линиям связи



244  
**ПРИЛОЖЕНИЕ Т**

**Расчет U-критерия Манна-Уитни для независимых выборок в IBM SPSS Statistics**



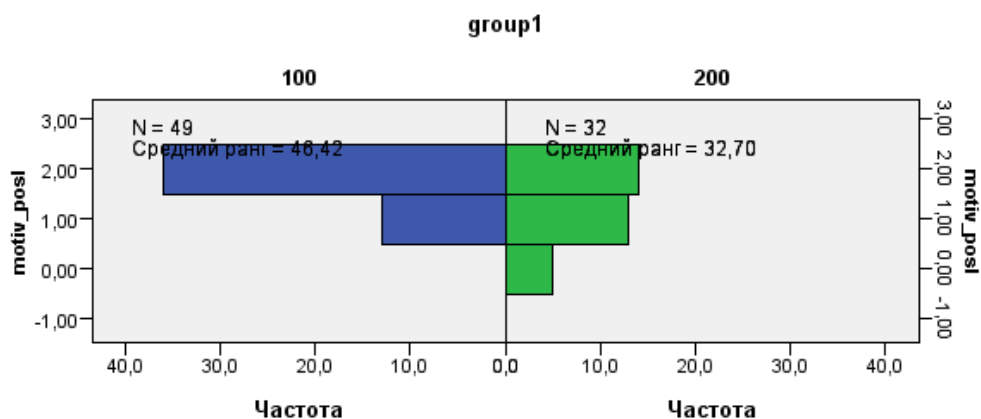
<b>Всего</b>	81
<b>U Манна-Уитни</b>	791,500
<b>W Уилкоксона</b>	1 319,500
<b>Статистика критерия</b>	791,500
<b>Стандартная ошибка</b>	93,934
<b>Стандартизованная статистика критерия</b>	,080
<b>Асимптотич. знч. (2-сторонний критерий)</b>	,936

Рисунок У.1 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню мотивационного критерия до проведения опытно-экспериментальной работы.

Таблица У.1 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню мотивационного критерия до проведения опытно-экспериментальной работы.

<b>Итоги по проверке гипотезы</b>				
	<b>Нулевая гипотеза</b>	<b>Критерий</b>	<b>Знач.</b>	<b>Решение</b>
<b>1</b>	Распределение motiv_kr является одинаковым для категорий group.		0,936	Нулевая гипотеза принимается.
Уровень значимости равен ,05.				

## Критерий U Манна-Уитни для независимых выборок



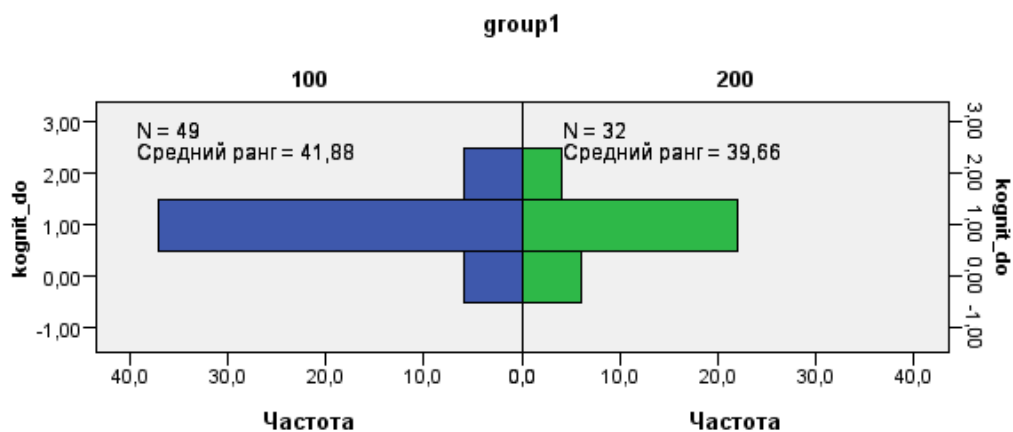
Всего	81
U Манна-Уитни	518,500
W Уилкоксона	1 046,500
Статистика критерия	518,500
Стандартная ошибка	88,537
Стандартизованная статистика критерия	-2,999
Асимптотич. знч. (2-сторонний критерий)	,003

Рисунок У.2 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню мотивационного критерия после проведения опытно-экспериментальной работы.

Таблица У.2 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню мотивационного критерия после проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение <i>motiv_posl</i> является одинаковым для категорий <i>group1</i> .	0,003	Нулевая гипотеза отклоняется.
Уровень значимости равен ,05.			

## Критерий U Манна-Уитни для независимых выборок

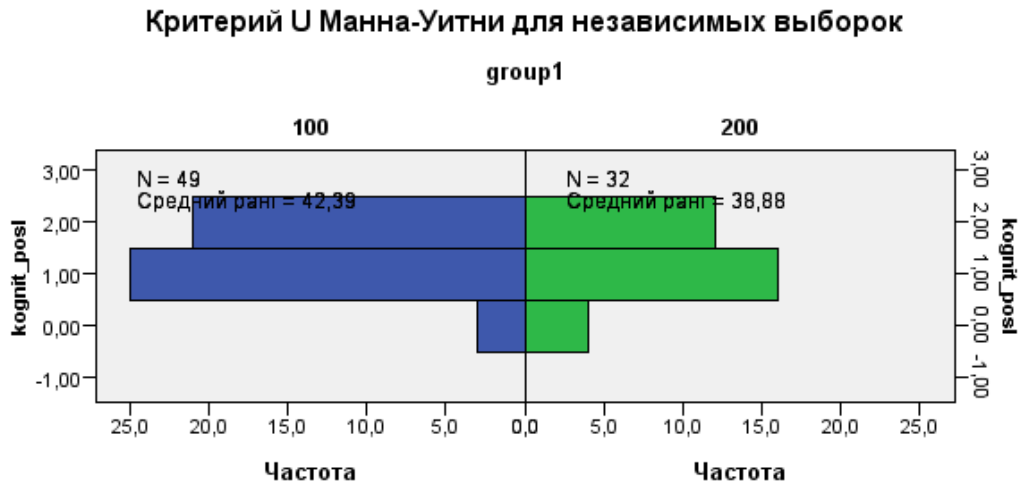


Всего	81
U Манна-Уитни	741,000
W Уилкоксона	1 269,000
Статистика критерия	741,000
Стандартная ошибка	80,746
Стандартизованная статистика критерия	-,533
Асимптотич. знч. (2-сторонний критерий)	,594

Рисунок У.3 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню когнитивного критерия до проведения опытно-экспериментальной работы.

Таблица У.3 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню когнитивного критерия до проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение <i>kognit_do</i> является одинаковым для категорий <i>group1</i> .	0,594	Нулевая гипотеза принимается.
. Уровень значимости равен ,05.			



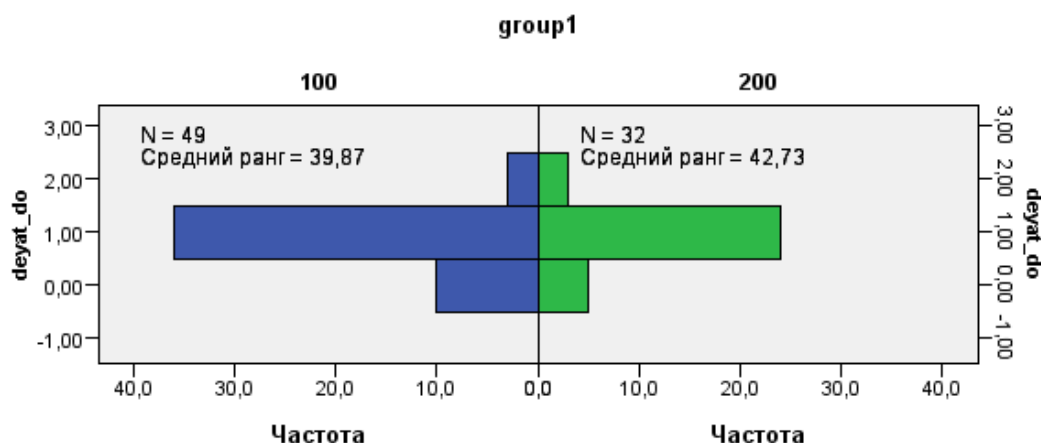
<b>Всего</b>	81
<b>U Манна-Уитни</b>	716,000
<b>W Уилкоксона</b>	1 244,000
<b>Статистика критерия</b>	716,000
<b>Стандартная ошибка</b>	92,709
<b>Стандартизованная статистика критерия</b>	-,733
<b>Асимптотич. знч. (2-сторонний критерий)</b>	,463

Рисунок У.4 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню когнитивного критерия после проведения опытно-экспериментальной работы.

Таблица У.4 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню когнитивного критерия после проведения опытно-экспериментальной работы.

<b>Итоги по проверке гипотезы</b>			
	<b>Нулевая гипотеза</b>	<b>Знач.</b>	<b>Решение</b>
<b>1</b>	Распределение <i>kognit_posl</i> является одинаковым для категорий <i>group1</i> .	0,463	Нулевая гипотеза принимается.
Уровень значимости равен ,05.			

## Критерий U Манна-Уитни для независимых выборок



Всего	81
U Манна-Уитни	839,500
W Уилкоксона	1 367,500
Статистика критерия	839,500
Стандартная ошибка	79,299
Стандартизованная статистика критерия	,700
Асимптотич. знч. (2-сторонний критерий)	,484

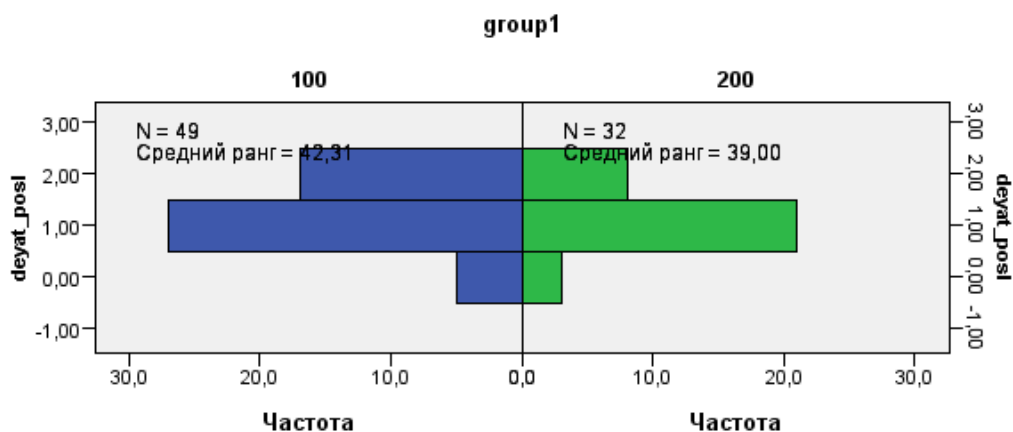
Рисунок У.5 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню деятельностного критерия до проведения опытно-экспериментальной работы.

Таблица У.5 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню деятельностного критерия до проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение deyat_do является одинаковым для категорий group1.	0,484	Нулевая гипотеза принимается.
Выводятся асимптотические значимости. Уровень значимости равен ,05.			



## Критерий U Манна-Уитни для независимых выборок



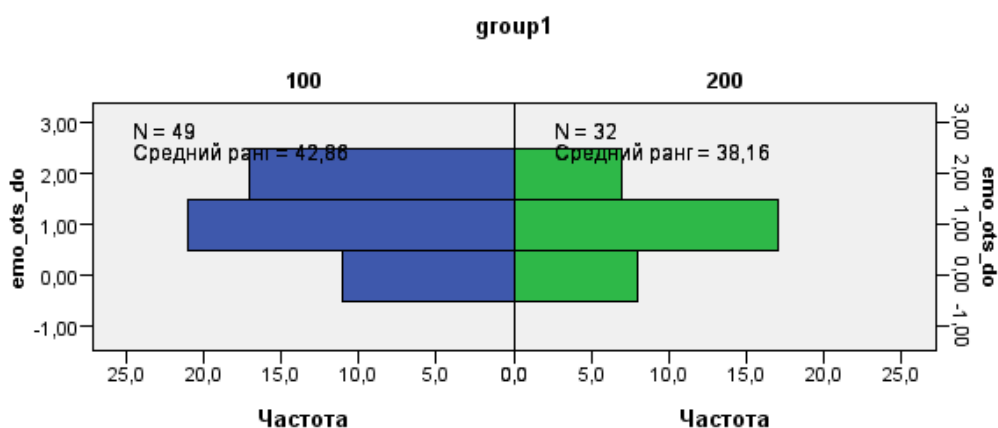
Всего	81
U Манна-Уитни	720,000
W Уилкоксона	1 248,000
Статистика критерия	720,000
Стандартная ошибка	90,337
Стандартизованная статистика критерия	-,708
Асимптотич. знч. (2-сторонний критерий)	,479

Рисунок У.6 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню деятельностного критерия после проведения опытно-экспериментальной работы.

Таблица У.6 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню деятельностного критерия после проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение <code>deyat_posl</code> является одинаковым для категорий <code>group1</code> .	0,479	Нулевая гипотеза принимается.
Уровень значимости равен ,05.			

## Критерий U Манна-Уитни для независимых выборок



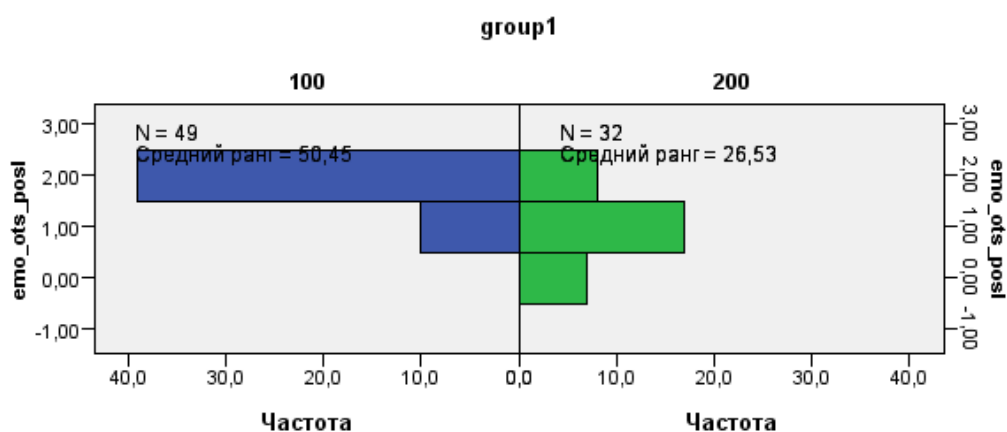
Всего	81
U Манна-Уитни	693,000
W Уилкоксона	1 221,000
Статистика критерия	693,000
Стандартная ошибка	95,879
Стандартизованная статистика критерия	-,949
Асимптотич. знч. (2-сторонний критерий)	,343

Рисунок У.7 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню эмоционально-оценочного критерия до проведения опытно-экспериментальной работы.

Таблица У.7 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню эмоционально-оценочного критерия до проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение emo_ots_do является одинаковым для категорий group1.	0,343	Нулевая гипотеза принимается.
Выводятся асимптотические значимости. Уровень значимости равен ,05.			

## Критерий U Манна-Уитни для независимых выборок



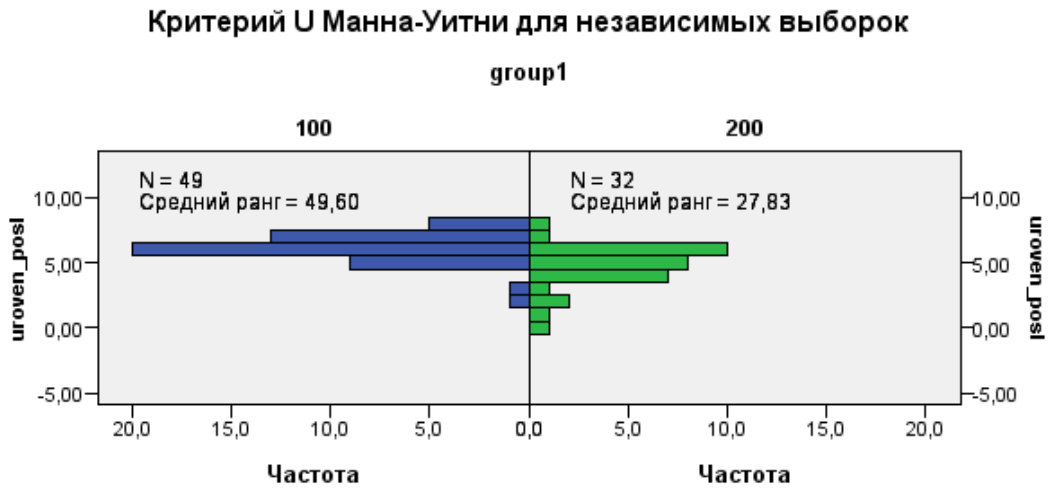
Всего	81
U Манна-Уитни	321,000
W Уилкоксона	849,000
Статистика критерия	321,000
Стандартная ошибка	90,658
Стандартизованная статистика критерия	-5,107
Асимптотич. знч. (2-сторонний критерий)	,000

Рисунок У.8 – Расчет U-критерия Манна-Уитни для независимых выборок КГ и ЭГ по уровню эмоционально-оценочного критерия после проведения опытно-экспериментальной работы.

Таблица У.8 – Итоги по проверке гипотезы для независимых выборок КГ и ЭГ по уровню эмоционально-оценочного критерия после проведения опытно-экспериментальной работы.

Итоги по проверке гипотезы			
	Нулевая гипотеза	Знач.	Решение
1	Распределение emo_ots_posl является одинаковым для категорий group1.	0	Нулевая гипотеза отклоняется.
Уровень значимости равен ,05.			





<b>Всего</b>	81
<b>U Манна-Уитни</b>	362,500
<b>W Уилкоксона</b>	890,500
<b>Статистика критерия</b>	362,500
<b>Стандартная ошибка</b>	100,027
<b>Стандартизованная статистика критерия</b>	-4,214
<b>Асимптотич. знч. (2-сторонний критерий)</b>	,000

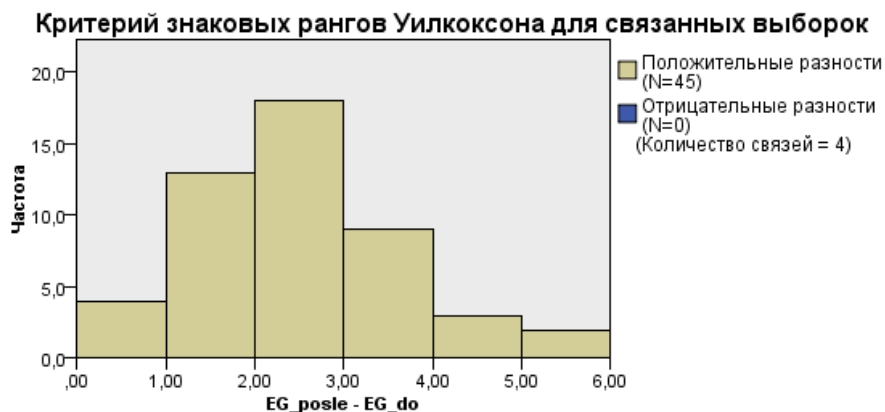
Рисунок У.10 – Расчет U-критерия Манна-Уитни для независимых выборок по уровню готовности на контрольном этапе.

Таблица У.10 – Итоги по проверке гипотезы для независимых выборок по уровню готовности на контрольном этапе

<b>Итоги по проверке гипотезы</b>			
	<b>Нулевая гипотеза</b>	<b>Знач.</b>	<b>Решение</b>
<b>1</b>	Распределение ugroven_posl является одинаковым для категорий group1.	0	Нулевая гипотеза отклоняется.
Уровень значимости равен ,05.			

## ПРИЛОЖЕНИЕ У

**Расчет критерия знаковых рангов Уилкоксона для связанных выборок  
в IBM SPSS Statistics**



<b>Всего</b>	49
<b>Статистика критерия</b>	1 035,000
<b>Стандартная ошибка</b>	87,559
<b>Стандартизованная статистика критерия</b>	5,910
<b>Асимптотич. знч. (2-сторонний критерий)</b>	,000

Рисунок Ф.1 – Расчет критерия знаковых рангов Уилкоксона для связанных выборок (ЭГ по уровню готовности к будущей профессиональной деятельности до и после проведения опытно-экспериментальной работы)

Таблица Ф.1 – Итоги по проверке гипотезы для связанных выборок (ЭГ по уровню готовности к будущей профессиональной деятельности до и после проведения опытно-экспериментальной работы)

<b>Итоги по проверке гипотезы</b>				
	<b>Нулевая гипотеза</b>	<b>Критерий</b>	<b>Знач.</b>	<b>Решение</b>
<b>1</b>	Медиана разностей между EG_do и EG_posle равна нулю.	Критерий знаковых рангов Уилкоксона для связанных выборок	0	Нулевая гипотеза отклоняется.
Уровень значимости равен ,05.				