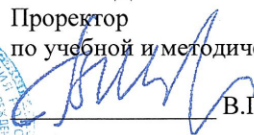


МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор
по учебной и методической работе




В.Г. Шубаева

«26» май 2021 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная
Год набора	2021

Санкт-Петербург
2021

1. Общие положения

1.1. Порядок проведения государственной итоговой аттестации (далее ГИА), состав и функции государственных экзаменационных комиссий и апелляционных комиссий, особенности проведения ГИА для выпускников из числа лиц с ограниченными возможностями регламентируется Положением о государственной итоговой аттестации выпускников ФГБОУВО «Санкт-Петербургский государственный экономический университет» (далее – СПбГЭУ, Университет).

1.2. Ответственность и порядок действий по подготовке и проведению государственных итоговых испытаний в СПбГЭУ, а также перечень, очередность, сроки прохождения документов, необходимых для осуществления государственной итоговой аттестации, между структурными подразделениями определяет Регламент организации государственной итоговой аттестации в «Санкт-Петербургском государственном экономическом университете».

1.3. Согласно требованиям ФГОС ВО 10.03.01 Информационная безопасность, в Блок 3 «Государственная итоговая аттестация», входит подготовка к процедуре защиты и защита выпускной квалификационной работы. Государственная итоговая аттестация проводится форме защиты выпускной квалификационной работы в виде дипломной работы.

1.4. Согласно требованиям ФГОС ВО общая трудоемкость государственной итоговой аттестации составляет 9 з.е. (324 ч.).

1.5. Результаты любого из видов аттестационных испытаний, включенных в государственную итоговую аттестацию, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

2. Цели и задачи государственной итоговой аттестации

2.1. Целью государственной итоговой аттестации является определение уровня подготовки выпускника к выполнению задач профессиональной деятельности и степени его соответствия требованиям ФГОС и результатам освоения ОПОП.

2.2. Основные задачи государственной итоговой аттестации направлены на проверку освоения следующих компетенций.

Код	Наименование компетенции выпускника
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)
УК-5	Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

Код	Наименование компетенции выпускника
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК-10.	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности
ОПК-4	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-7	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
ОПК-13	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма
ОПК-1.1	Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах
ОПК-1.2	Способен администрировать средства защиты информации в компьютерных системах и сетях
ОПК-1.3	Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям
ОПК-1.4	Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями

Код	Наименование компетенции выпускника
ПК-1	Способен управлять функционированием программно-аппаратных средств защиты информации в компьютерных системах и сетях
ПК-2	Способен производить установку и конфигурирование средств защиты информации в операционных системах, включая средства криптографической защиты информации
ПК-3	Способен формулировать требования к средствам защиты информации прикладного и системного программного обеспечения
ПК-4	Способен выявлять уязвимости системы защиты информации в процессе разработки и внедрения компьютерных систем
ПК-5	Способен выявлять угрозы безопасности информации и анализировать недостатки функционирования системы защиты информации на объектах информатизации
ПК-6	Способен выявлять и идентифицировать инциденты в процессе эксплуатации автоматизированных систем
ПК-7	Способен организовывать выполнение политик безопасности и обеспечивать применение организационных мер защиты информации на объекте информатизации
ПК-8	Способен разрабатывать организационно-распорядительные документы по защите информации на объектах информатизации

3. Характеристика профессиональной деятельности выпускников

Область (-и) профессиональной деятельности и (или) сфера (-ы) профессиональной деятельности:

06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

Типы задач и задачи профессиональной деятельности:

- эксплуатационный;
- проектно-технологический;
- экспериментально-исследовательский
- организационно-управленческий.

4. Требования к выпускной квалификационной работе

4.1. Перечень тем дипломных работ

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).

6. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
8. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
10. Разработка методологии проектирования КСЗИ.
11. Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
14. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).
15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия).
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).
18. Разработка изолированной программно-аппаратной среды в Windows NT (WINDOWS 20xx, LINUX и т.д.) (наименование предприятия).
19. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
20. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
21. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
22. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
23. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
24. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
25. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
26. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
27. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
28. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
29. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при

- вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
30. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
 31. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации (название предприятия).
 32. Организация автоматизированного пропускного режима на крупном предприятии (на примере).
 33. Разработка проекта организационных мер по защите аудиоинформации в локальной сети (название предприятия).
 34. Разработка комплексной системы защиты информации в кабинете директора (название предприятия).
 35. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
 36. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия).
 37. Разработка организационного порядка установления внутриобъектного режима для торговой фирмы (название предприятия).
 38. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
 39. Построение алгоритма системы идентификации, защищенной от подделки продукции.
 40. Организация системы контроля доступа и защиты информации на предприятии (на примере ООО «Передвижная механизированная колонна-4»).
 41. Разработка комплексной системы защиты информации в кабинете руководителя предприятия.
 42. Защита речевой информации в каналах связи коммерческих организаций.
 43. Разработка проекта корпоративной сети (название предприятия).
 44. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
 45. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации для (название предприятия).
 46. Анализ методов и форм работы с персоналом, допущенным к конфиденциальной информации, и разработка рекомендаций по их применению для торговых организаций.
 47. Разработка подсистемы защиты от НСД для мобильных устройств предприятия.
 48. Разработка подсистемы криптографической защиты информации, передаваемой по каналам связи для мобильных устройств.
 49. Организация подсистемы резервного копирования (название предприятия)
 50. Анализ методов оценки защищенности ERP-систем
 51. Разработка системы мониторинга и анализа защищенности сети (название предприятия).

4.2. Задачи, которые студент должен решить в процессе выполнения выпускной квалификационной работы, этапы ее выполнения, условия допуска студента к процедуре защиты, требования к структуре, объему, содержанию и оформлению, а также перечень обязательных и рекомендуемых документов, представляемых к защите указаны в Методических указаниях, утвержденных в установленном порядке.

5. *Фонд оценочных средств государственной итоговой аттестации*

Фонд оценочных средств для проведения государственной итоговой аттестации оформляется отдельным документом и является приложением к программе государственной итоговой аттестации.

6. *Материально-техническое обеспечение государственной итоговой аттестации*

Для реализации государственной итоговой аттестации Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение ГИА. Имеющееся материально-техническое обеспечение в полном объеме и на уровне современных требований позволяет организовать ГИА Университета. При необходимости использования соответствующего ПО для написания ВКР, обучающимся, может быть предоставлен доступ к ПО в соответствующих аудиториях.

7. *Особенности проведения государственной итоговой аттестации для лиц с ограниченными возможностями здоровья*

Для обучающихся из числа инвалидов государственная итоговая аттестация проводится организацией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья в соответствии с Положением «О государственной итоговой аттестации выпускников федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный экономический университет»».