Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный технический университет им. И. И. Ползунова»

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по образовательной программе бакалавриата

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Направленность (профиль) Организация и технология защиты информации

	Должность	И.О. Фамилия	Подпись
Разработал	Доцент кафедры ИВТиИБ	Е.В. Шарлаев	
Согласовал	Зав. кафедрой	А.Г. Якунин	
	Руководитель ОП	Е.В. Шарлаев	
	Декан (директор)	А.С. Авдеев	

Барнаул

1 Общие положения

Целью государственной итоговой аттестации является определение соответствия результатов освоения обучающимися образовательной программы по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль) Организация и технология защиты информации) соответствующим требованиям федерального государственного образовательного стандарта высшего образования (ФГОС ВО), утверждённого от 1 декабря 2016 г. N 1515.

1.1 Форма и сроки проведения государственной итоговой аттестации

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы (ВКР), включая подготовку к процедуре защиты и процедуру защиты.

Сроки проведения государственной итоговой аттестации определяются образовательными программами (ОП) в пределах норм, установленных соответствующими ФГОС ВО, фиксируются в учебных планах в разделе «Календарный учебный график».

1.2 Определение содержания государственной итоговой аттестации

1.2.1 Образовательной программой по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль) Организация и технология защиты информации) предусматривается подготовка выпускников к следующим видам профессиональной деятельности:

эксплуатационная;
проектно-технологическая;
экспериментально-исследовательская;
организационно-управленческая.

1.2.2 Требования к результатам освоения ОП

Перечень компетенций, которыми должен обладать выпускник в результате освоения ОП:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);

способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3);

способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);

способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности (ОПК-6);

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

способностью проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК2-1);

способностью формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК2-2);

способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК2-3);

способностью организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК2-4).

2 Требования к выпускной квалификационной работе

По итогам выпускной квалификационной работы проверяется степень освоения обучающимися компетенций.

Общие требования к содержанию и оформлению ВКР, порядок выполнения и представления ВКР к защите в ГЭК, порядок защиты и критерии оценивания ВКР, а также порядок подачи и рассмотрения апелляций определяются локальными нормативными актами АлтГТУ. Структура ВКР и другие требования по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль) Организация и технология защиты информации) определяются учебно-методическими материалами профилирующей кафедры.

Примерная тематика ВКР соответствует видам профессиональной деятельности:

- эксплуатационная деятельность:
    1. Организация защищенной виртуальной частной сети на основе различных программно-аппаратных комплексов защиты информации.
    2. Модернизация элементов комплексной защиты предприятий различных типов собственности и видов деятельности.
    3. Разработка АРМ специалиста по защите информации для объектов информатизации различных сфер деятельности.
    4. Обеспечение безопасности облачных серверов на основе UNIX-систем.
    5. Обеспечение антивирусной защиты на объектах информатизации.
    6. Разработка эксплуатационной документации для программно-аппаратных средств защиты информации.
- проектно-технологическая деятельность:
    1. Разработка проектов защищенной локально-вычислительной сети (ЛВС) для предприятия с учетом основной деятельности и особенностей размещения автоматизированного рабочего места (АРМ).
    2. Разработка проектов внедрения новых или замены устаревших средств защиты сетевой инфраструктуры в существующие ЛВС.
    3. Разработка проектов модернизации ЛВС с целью недопущения ослабления

(снижения) степени защищенности системы.
4. Разработка проектной документации с целью детального описания аппаратуры и настроек средств сетевой защиты.
5. Разработка протоколов безопасного сетевого взаимодействия и разработка новых способов и методов безопасного использования существующих протоколов.

- экспериментально-исследовательская деятельность:
1. Разработка принципиально новых методик оценки защищенности с использованием инновационных методов и технологий.
2. Разработка средств обнаружения вторжений в компьютерные системы.
3. Поиск уязвимостей алгоритмов шифрования, описание методов взлома.
4. Исследование свойств систем и сетей связи.

- организационно-управленческая деятельность:
1. Разработка рекомендаций по менеджменту рисков информационной безопасности в органах власти.
2. Разработка рекомендаций по обеспечению безопасности персональных данных.
3. Разработка документов по организации функционирования удостоверяющего центра.
4. Разработка рекомендаций по использованию электронной подписи в органах власти.

3 Фонд оценочных материалов государственной итоговой аттестации

Фонд оценочных материалов государственной итоговой аттестации включает перечень вопросов для оценки степени сформированности компетенций:

1. Оцените, насколько тема и содержание ВКР позволяют выразить Вашу личную мировоззренческую позицию или позволяют повлиять на мировоззренческую позицию других? (ОК-1)
2. Какие философские проблемы и методы нашли отражение в ВКР? (ОК-1)
3. Как экономические знания использовались при подготовке ВКР? (ОК-2)
4. Назовите основные критерии при оценке экономической эффективности результатов ВКР (ОК-2)
5. Какие основные этапы исторического развития Вы знаете? (ОК-3)
6. Как анализ этапов и закономерностей исторического развития влияет на формирование гражданской позиции? (ОК-3)
7. Какова роль России в современном мире? (ОК-3)
8. Какие основы правовых знаний использовались при выполнении ВКР? (ОК-4)
9. Насколько правовые знания актуальны для достижения успеха в профессиональной деятельности? (ОК-4)
10. Какую социальную значимость имеет Ваша будущая профессия? (ОК-5)
11. Поясните Вашу мотивацию к выполнению профессиональной деятельности в области информационной безопасности (ОК-5)
12. Какие нормы профессиональной этики в будущей профессии Вы знаете? (ОК-5)
13. Как Вы оцениваете свою способность работать в коллективе? (ОК-6)
14. Как учитываются социальные, этнические, конфессиональные и культурные различия при работе в команде? (ОК-6)
15. Какие формы коммуникации Вы использовали при выполнении ВКР? (ОК-7)
16. Какие тексты были Вами переведены с иностранного (-ых) на государственный язык и с государственного на иностранный (-ые) язык(и) при выполнении ВКР? (ОК-7)

17. Как Вы оцениваете результаты межличностного и межкультурного взаимодействия при выполнении ВКР? (ОК-7)
18. Какие приемы самоорганизации использовались при выполнении ВКР? (ОК-8)
19. Насколько самообразование помогло Вам достичь цели ВКР? (ОК-8)
20. Перечислите факторы, влияющие на здоровье и физическую подготовку человека (ОК-9)
21. Какие средства физической культуры Вы используете для сохранения и укрепления здоровья? (ОК-9)
22. Оцените Ваш уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (ОК-9)
23. Какие законы физики применимы к области технической защиты информации? (ОПК-1)
24. Какие физические явления и процессы лежат в основе работы инфракрасных извещателей систем охранной сигнализации? (ОПК-1)
25. В чем отличие Ваших алгоритмов от уже известных? (ОПК-2)
26. Поясните, какой математический аппарат используется при оценке рисков информационной безопасности в организации и каков практический опыт его применения? (ОПК-2)
27. Какие положения электротехники, электроники и схемотехники применялись для решения поставленных задач? (ОПК-3)
28. Какие схемотехнические решения используются в акустических извещателях систем охранной сигнализации? (ОПК-3)
29. Какое место занимают вопросы защиты информации в современном обществе? (ОПК-4)
30. Какие сайты профессиональной направленности Вы периодически посещаете?
31. (ОПК-4)
32. Какие нормативные правовые акты Вы использовали для решения задач, поставленных в работе? (ОПК-5)
33. Приведите правовое обоснование для сформированного Вами комплекса мер по информационной безопасности. (ОПК-5)
34. Перечислите мероприятия по технике безопасности при работе с излучающими техническими средствами защиты информации (ОПК-6)
35. Определите алгоритм действий специалистов IT-отделов в случаях возникновения аварийной или чрезвычайной ситуации (ОПК-6)
36. Приведите правовое обоснование для сформированного Вами комплекса мер по информационной безопасности. (ОПК-7)
37. Какие угрозы информационной безопасности характерны только для объектов рассматриваемого Вами предприятия, обусловленные спецификой его деятельности? (ОПК-7)
38. Обзор каких средств защиты вы провели и как он повлиял на выбор средств, используемых в Вашей работе? (ОПК-7)
39. Какие программно-аппаратные средства защиты использованы в разработке? (ПК-1)
40. В чем состоит особенность работ по установке, настройке и обслуживанию криптографических средств защиты информации? (ПК-1)
41. Какие инструментальные средства и системы программирования были проанализированы для решения Ваших задач? (ПК-2)
42. Поясните выбор среды разработки ПО, в чем ее достоинства и недостатки? (ПК-2)
43. Какие особенности администрирования разработанной Вами подсистемы информационной безопасности? (ПК-3)

44. Какие компетенции требуются от администратора подсистем информационной безопасности объекта защиты? (ПК-3)
45. В чем заключается комплексный подход к обеспечению информационной безопасности объекта защиты? (ПК-4)
46. Назовите основные мероприятия при проведении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)
47. Какие нормативные правовые акты и стандарты используются в ходе выполнения аттестации объектов информатизации? (ПК-5)
48. Почему вы выполнили программную реализацию криптографического алгоритма именно на этом языке программирования? (ПК-6)
49. Перечислите основные критерии эффективности функционирования защищенных информационных систем (ПК-6)
50. Какие инструментальные средства и системы программирования были проанализированы для решения Ваших задач? (ПК-7)
51. Назовите основные этапы и порядок проектирования защищённых информационных систем (ПК-7)
52. Какие нормативные и методические документы в области информационной безопасности вы использовали при разработке технической документации? (ПК-8)
53. Как организовывается работа по сертификации средств защиты информации на объекте информатизации? (ПК-8)
54. На основе каких критериев или принципов Вы осуществили выбор (изучение и обобщение научно-технической литературы), нормативных и методических материалов для решения вопроса обеспечения информационной безопасности? (ПК-9)
55. Какие основные электронные базы научно-технической литературы в области ИБ и защиты информации использовались в процессе подготовки и написания ВКР? (ПК-9)
56. Какие методы анализа уязвимостей и угроз вы использовали в интересах разработки проектных решений? (ПК-10)
57. Назовите наиболее известные отечественные и зарубежные стандарты для оценки защищённости компьютерных систем (ПК-10)
58. Какие предложения по совершенствованию системы управления информационной безопасностью разработаны лично? (ПК-11)
59. Какими методами проведен расчет показателей технической защиты информации защищаемого объекта информатизации? (ПК-11)
60. Перечислите наиболее эффективные способы и средства защиты информации от утечки по техническим каналам (ПК-12)
61. Какие экспериментальные исследования разработанной системы защиты информации проведены лично Вами? (ПК-12)
62. Какие элементы включает подсистема управления информационной безопасностью в рассматриваемой Вами работе (организации). (ПК-13)
63. Как обеспечивается организация и управление деятельностью служб защиты информации на объекте информатизации? (ПК-13)
64. Перечислите основные должностные обязанности руководителя отдела защиты информации предприятия (организации) (ПК-14)
65. Что, по Вашему мнению, составляет содержание управленческой работы руководителя подразделения по обеспечению информационной безопасности? (ПК-14)
66. Какие нормативно-правовые документы лежат в основе организации технологического процесса защиты информации ограниченного доступа? (ПК-15)

67. Какие требования предъявляются к помещениям, предназначенным для хранения документов ограниченного доступа? (ПК-15).
68. Какие исходные данные положены в основу Вашего проектного решения подсистемы (средства) обеспечения информационной безопасности. (ПСК2-1)
69. Как в работе реализован комплексный подход к обеспечению информационной безопасности и как в нём учтена специфика деятельности предприятия? (ПСК2-1)
70. Какие предложения сформированы Вами по тактике защиты объекта и локализации защищаемых элементов? (ПСК2-2)
71. Какие результаты дал предварительный технико-экономический анализ компонентов (системы) защиты организации и как он повлиял на обоснование проектного решения по обеспечению информационной безопасности? (ПСК2-2)
72. Что включает предложенный Вами комплекс мер по обеспечению информационной безопасности объекта в части организационной составляющей? (ПСК2-3)
73. Как планируется организовать внедрение и последующее сопровождение предложенного Вами комплекса мер по обеспечению информационной безопасности объекта в части организационной составляющей? (ПСК2-3)
74. Какие нормативные документы используются в процессе организации контроля защищенности объекта информатизации? (ПСК2-4)
75. Какие современные методики контроля защищенности объекта информатизации наиболее эффективны и почему? (ПСК2-4).