Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт экономики, математики и информационных технологий
Центр «Школа IT-менеджмента»
(наименование структурного подразделения)

«УТВЕРЖДАЮ»
Заместитель директора
Института ЭМИТ
С.А. Маруев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 518ECD0030B34FA54703CB5018048863
Владелец: Маруев Сергей Александрович
Действителен: с 05.08.2025 до 05.08.2026

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации

«Комплексное обеспечение информационной безопасности автоматизированных систем»
(наименование программы)

Москва, 2026

Разработчик и руководитель программы

Директор программы Центр «Школа ИТ-менеджмента», Институт экономики, математики и информационных технологий  Т.Е. Соколова

Программа повышения квалификации рассмотрена на заседании ученого совета Института экономики, математики и информационных технологий и рекомендована к реализации, протокол № 5 от «18» февраля 2026 г.

Федеральное государственное бюджетное образовательное учреждение высшего образования Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

Институт экономики, математики информационных технологий

(наименование структурного подразделения)

ВЫПИСКА ИЗ ПРОТОКОЛА

заседания ученого совета ИЭМИТ

от «18» февраля 2026 г. **№ 5**

Москва

Председатель – Радыгин Александр Дмитриевич

Ученый секретарь – Шорникова Наталья Юрьевна

Повестка дня:

1. Утверждение ДПП ПК «Комплексное обеспечение информационной безопасности автоматизированных систем»
2. Утверждение ДПП ПК «Цифровая трансформация для IT-руководителей»
3. Утверждение ДПП ПП «Мастер делового администрирования – Master of Business Administration (MBA) "IT-Лидер (CIO, CISO, CDO)"»

СЛУШАЛИ:

Соколова А.И., директора Центра «Школа IT-менеджмента» ИЭМИТ. На обсуждение представлены ДПП ПК «Комплексное обеспечение информационной безопасности автоматизированных систем», ДПП ПК «Цифровая трансформация для IT-руководителей», ДПП ПП «Мастер делового администрирования – Master of Business Administration (MBA) "IT-Лидер (CIO, CISO, CDO)"»

ПОСТАНОВИЛИ:

Рекомендовать к реализации дополнительные профессиональные программы повышения квалификации и профессиональной переподготовки:

- «Комплексное обеспечение информационной безопасности автоматизированных систем»
- «Цифровая трансформация для IT-руководителей»
- «Мастер делового администрирования – Master of Business Administration (MBA) "IT-Лидер (CIO, CISO, CDO)"»

Председатель ученого совета Института ЭМИТ _____ А.Д. Радыгин

Секретарь ученого совета Института ЭМИТ _____ Н.Ю. Шорникова

ВНУТРЕННЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации
«Комплексное обеспечение информационной безопасности автоматизированных систем»
(наименование программы)

Категория слушателей программы - Руководители высшего и среднего звена в области информационной безопасности, подразделений по защите информации, информационных технологий, сотрудники частных компаний и государственных организаций, которым требуется повышение профессионального уровня в области информационной безопасности в соответствии с актуальными изменениями в вопросах защиты информации, имеющие высшее образование (бакалавр, дипломированный специалист, магистр).

Актуальность программы - Программа направлена на повышение квалификации руководителей и специалистов в области корпоративной информационной безопасности, способных грамотно и на современном уровне строить систему противодействия угрозам деятельности компании.

Цель программы: Целью программы является получение теоретических знаний и практических навыков, а также повышение квалификации слушателей и подготовка их к последующей практической работе по менеджменту в области обеспечения информационной безопасности автоматизированных систем, локальных и корпоративных информационных сетей, а также при подключении к информационно-вычислительным сетям общего назначения, в том числе к сети Internet. Знакомство с последними изменениями в законодательстве Российской Федерации и международных стандартов безопасности.

Основное направление подготовки: 38.04.02 «Менеджмент»

Особенности программы: В последние годы круг обязанностей и компетенций директора по информационной безопасности сильно изменился. Теперь уже недостаточно быть продвинутым ИТ-специалистом с функциями специалиста по информационной безопасности. Обеспечение информационной безопасности и организация защиты информации требуют постоянного внимания. Постоянно появляются новые угрозы и развиваются новые технологии, растет число вредоносных программ и усложняются способы обеспечения безопасности IT-инфраструктуры. Все это предъявляет к CSO более высокие требования и не только к знаниям новых технологий, возможных угроз и рисков, которые они несут, но и личностных и управленческих качеств для быстрого реагирования на изменения в системе безопасности компании. Обеспечение информационной безопасности компании состоит не только в организации защиты информации, но и в профессиональном подходе к обучению специалистов.

Срок реализации программы: Вечерний формат обучения: срок обучения - 13 недель, режим занятий – два-три вечера в неделю с 19.00 до 22.00 и суббота с 09.00 до 17.10; модульный формат обучения – 5 недель и 5 дней (очный модуль 10 дней), режим занятий - с 09.00 до 17.10.

Заключение:

В современном быстро развивающемся и быстро меняющемся мире стремительное развитие информационных технологий влечет за собой постоянное изменение характера угроз корпоративных данных. В частности, получили широкое распространение средства несанкционированного доступа к информации. Каждое предприятие, обладающее конфиденциальной информацией, предпринимает серьезные меры по сохранению конфиденциальной информации: защита конфиденциальной информации в условиях жесточайшей конкурентной борьбы стала ключевой задачей ИТ-специалистов.

Своевременный анализ системы информационной безопасности может существенно сократить риски воздействия на информацию. Для этого нужны специалисты, качественно подготовленные по данному профилю. Именно поэтому повышение квалификации кадров в сфере информационных технологий и информационной безопасности является очень востребованным направлением.

К рассмотрению была предложена программа повышения квалификации «Комплексное обеспечение информационной безопасности автоматизированных систем». Явным преимуществом программы является ее преподавательский состав: здесь преподают практики, успешные топ-менеджеры и консультанты, имеющие большой практический опыт. Безусловно, высококвалифицированный преподавательский состав является залогом качества подготовки специалистов, обладающих современными навыками построения системы противодействия угрозам деятельности компании.

В программу заложен базис, включающий в себя такие дисциплины как «Формирование и реализация политики обеспечения информационной безопасности», «Эффективность защиты информации», «Организация защиты персональных данных» и другие. В процессе обучения слушатель получает не только теоретические знания, но и комплексные практические навыки по созданию надежной системы информационной безопасности в своей компании. В ходе прохождения программы слушатели изучают правовые и организационные основы обеспечения безопасности в информационных системах персональных данных, методы и процедуры выявления угроз безопасности и оценки степени их опасности. В рамках практических занятий отрабатываются навыки в проведении мероприятий по обеспечению защиты персональных данных при их обработке в информационной системе персональных данных.

Программа соответствует требованиям, предъявляемым к дополнительным профессиональным программам повышения квалификации и рекомендуется к реализации.

Рецензент  Гадзаов Ф. Директор центра "Цифровая школа госуправления" ВШГУ РАНХиГС, к.э.н.

ВНЕШНЯЯ РЕЦЕНЗИЯ

на дополнительную профессиональную программу повышения квалификации
«Комплексное обеспечение информационной безопасности автоматизированных систем»
(наименование программы)

Категория слушателей программы - Руководители высшего и среднего звена в области информационной безопасности, подразделений по защите информации, информационных технологий, сотрудники частных компаний и государственных организаций, которым требуется повышение профессионального уровня в области информационной безопасности в соответствии с актуальными изменениями в вопросах защиты информации, имеющие высшее образование (бакалавр, дипломированный специалист, магистр).

Актуальность программы - Программа направлена на повышение квалификации руководителей и специалистов в области корпоративной информационной безопасности, способных грамотно и на современном уровне строить систему противодействия угрозам деятельности компании.

Цель программы: Целью программы является получение теоретических знаний и практических навыков, а также повышение квалификации слушателей и подготовка их к последующей практической работе по менеджменту в области обеспечения информационной безопасности автоматизированных систем, локальных и корпоративных информационных сетей, а также при подключении к информационно-вычислительным сетям общего назначения, в том числе к сети Internet. Знакомство с последними изменениями в законодательстве Российской Федерации и международных стандартов безопасности.

Основное направление подготовки: 38.04.02 «Менеджмент»

Особенности программы: В последние годы круг обязанностей и компетенций директора по информационной безопасности сильно изменился. Теперь уже недостаточно быть продвинутым ИТ-специалистом с функциями специалиста по информационной безопасности. Обеспечение информационной безопасности и организация защиты информации требуют постоянного внимания. Постоянно появляются новые угрозы и развиваются новые технологии, растет число вредоносных программ и усложняются способы обеспечения безопасности IT-инфраструктуры. Все это предъявляет к CSO более высокие требования и не только к знаниям новых технологий, возможных угроз и рисков, которые они несут, но и личностных и управленческих качеств для быстрого реагирования на изменения в системе безопасности компании. Обеспечение информационной безопасности компании состоит не только в организации защиты информации, но и в профессиональном подходе к обучению специалистов.

Срок реализации программы: Вечерний формат обучения: срок обучения - 13 недель, режим занятий – два-три вечера в неделю с 19.00 до 22.00 и суббота с 09.00 до 17.10; модульный формат обучения – 5 недель и 5 дней (очный модуль 10 дней), режим занятий - с 09.00 до 17.10.

Заключение:

Программа повышения квалификации «Комплексное обеспечение информационной безопасности» представляет собой краткосрочный курс, предназначенный для максимально продуктивного ознакомления менеджеров высшего и среднего звена в области информационной безопасности с актуальными изменениями в вопросах защиты информации, ведь способы обеспечения безопасности IT-инфраструктуры постоянно усложняются.

Длительность программы составляет 314 академических часов. В ее состав входит набор таких актуальных дисциплин как «Стандарты и аудит информационной безопасности ISO 27001», «Организация защиты персональных данных и связанные с этим мероприятия», «Формирование и реализация политики обеспечения информационной безопасности», «Защита критической информационной инфраструктуры», «Криптографическая защита информации», «Организация защиты персональных данных», «Эффективность защиты информации», «Законодательство информационной безопасности», «Комплексное обеспечение информационной безопасности в интернет». Программу можно назвать емкой: за достаточно небольшой промежуток времени слушателю будет раскрыт широкий спектр вопросов.

Программа имеет практическую ориентацию: помимо тренингов, на занятиях проводится разбор практических задач по месту основной работы слушателей. Кроме того, программа предусматривает часы для выполнения самостоятельной работы слушателей. По выполнению самостоятельной работы слушатель получает обратную связь от преподавателя, что делает процесс обучения наиболее эффективным.

Программа соответствует требованиям, предъявляемым к дополнительным профессиональным программам повышения квалификации и рекомендуется к реализации.

Рецензент _____ .(подпись)

Линник В.
зам. д-р АРСИБ
(ФИО, должность, ученая степень, ученое звание)

Российская Федерация * Ассоциация руководителей служб информационной безопасности * АРСИБ ДЛЯ ДОКУМЕНТОВ Москва * ОГРН 1227700369210

СОДЕРЖАНИЕ

1. Общая характеристика программы 5
1.1. Цель реализации программы 5
1.2. Нормативные правовые акты 5
1.3. Планируемые результаты обучения 6
1.4. Категория слушателей 8
1.5. Формы и технологии обучения 9
1.6. Период обучения, срок освоения и режим занятий 9
1.7. Документ о квалификации 9
2. СОДЕРЖАНИЕ ПРОГРАММЫ 10
2.1. Календарный учебный график 10
2.2. Содержание программы по дисциплинам 12
3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ 13
3.1. Материально-техническое и программное обеспечение реализации программы 13
3.2. Учебно-методическое и информационное обеспечение программы 13
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ 18
5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ 28

Приложение 1. Сведения о профессорско-преподавательском составе и ведущих специалистах (кадровая справка)[1]

[1] Кадровая справка не входит в состав программы и формируется отдельно

1. Общая характеристика программы

1.1. Цель реализации программы

Программа направлена на повышение квалификации руководителей и специалистов в области корпоративной информационной безопасности, способных грамотно и на современном уровне строить систему противодействия угрозам деятельности компании.

Целью программы является получение теоретических знаний и практических навыков, а также повышение квалификации слушателей и подготовка их к последующей практической работе по менеджменту в области обеспечения информационной безопасности автоматизированных систем, локальных и корпоративных информационных сетей, а также при подключении к информационно-вычислительным сетям общего назначения, в том числе к сети Internet. Знакомство с последними изменениями в законодательстве Российской Федерации и международных стандартов безопасности.

1.2. Нормативные правовые акты

1. Общероссийский классификатор занятий (Приказ Федерального агентства по техническому регулированию и метрологии от 12 декабря 2014 г. N 2020-ст)
2. Единый квалификационный справочник должностей руководителей, специалистов и других служащих 4-е издание, дополненное (утв. постановлением Минтруда РФ от 21 августа 1998 г. N 37) (с изменениями и дополнениями)
3. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
4. Приказ Министерства науки и высшего образования РФ от 24 марта 2025 г. N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".
5. Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ Министерства образования и науки Российской Федерации от 10.04.2014 года № 06-381.
6. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов. ОК 016-2025» (ОКПДТР), утверждённый приказом Росстандарта от 16.05.2025 №423-ст.
7. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», Приказ Минтруда и социальной защиты РФ от 14.09.2022 N 525н
8. Общероссийский классификатор видов экономической деятельности (утв. Приказом Росстандарта от 31.01.2014 N 14-ст) (ред. от 11.19.2025)
9. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.04.02 Менеджмент (уровень магистратуры) (утв. Приказом Минобрнауки РФ от 12 августа 2020 г. N 952)
10. Приказ РАНХиГС «Об утверждении локальных нормативных актов РАНХиГС по дополнительному профессиональному образованию» №02-461 от 19 апреля 2019 года
11. Приказ РАНХиГС от 22 сентября 2017 года №01-6230 «Об утверждении Положения о применении в Академии электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».
12. Приказ Академии от 02 декабря 2025 года № «02»-02669/001 «Об утверждении порядка разработки и утверждения в Академии дополнительных профессиональных программ – программ повышения квалификации, программ профессиональной переподготовки»
13. Приказ Академии от 13 января 2026 года № 02-00010/001 «Об утверждении Правил

приема на обучение по дополнительным программам в Академию»

14. Приказ Академии от 13 января 2026 года № 02-00009/001 «Об утверждении Положения об итоговой аттестации слушателей дополнительных программ в Академии»

1.3. Планируемые результаты обучения

Таблица 1

Перечень профессиональных компетенций в рамках имеющейся квалификации и профессиональных компетенций, планируемых к освоению (результаты обучения)

Виды деятельности	**Общепрофессиональные/профессиональные компетенции ОПК, ПК или трудовые функции (ПСК и СК)** ***(формируются и (или) совершенствуются)***	**Практический опыт**	**Знания**	**Умения**
1	**2**	**3**	**4**	**5**
Организационно-управленческая деятельность	Способен самостоятельно принимать обоснованные организационно-управленческие решения, оценивать их операционную, социальную значимость, обеспечивать их реализацию в условиях сложной (в том числе кросс-культурной) и динамичной среды (ОПК-3)	Навыки управленческой деятельности в различных сферах экономики на международном рынке посредством производных инструментов	Знание современных стилей и моделей управления сотрудниками; инновационных подходов управления организациями	Умение применять современные методы руководства на различных иерархических уровнях управления
Обеспечение безопасности информации в автоматизированных системах	Способность обоснования необходимости защиты информации в автоматизированной системе (ПСК-1)	Формирование и согласование стратегических целей цифровой трансформации в организации, регионе, стране Организация управления разработкой и обновлением цифровой стратегии развития организации, региона, страны с помощью персонала и стейкхолдеров	Международные и отечественные стандарты, лучшие практики и фреймворки по разработке и реализации цифровой стратегии организации (региона, страны) Методы организации разработки и реализации цифровой стратегии организации	Формировать и согласовывать стратегические цели цифровой трансформации со стейкхолдерами Организовывать деятельность по разработке и выполнению цифровой стратегии организации (региона, страны) Осуществлять мониторинг и контроль разработки и выполнения цифровой стратегии

		Организация и выполнение цифровой стратегии организации (региона, страны) с помощью персонала и стейкхолдеров Контроль и мониторинг разработки и выполнения цифровой стратегии организации (региона, страны)	(региона, страны)	организации (региона, страны)
	Способность определения угроз безопасности информации, обрабатываемой автоматизированной системой (ПСК-2)	Формирование и согласование принципов управления программами и портфелями ИТ-проектов Организация управления программами и портфелями ИТ-проектов с помощью персонала и стейкхолдеров Контроль качества и управление улучшением управления программами и портфелями ИТ-проектов	Международные и отечественные стандарты, лучшие практики и фреймворки по управлению портфелями проектов Международные и отечественные стандарты, лучшие практики и фреймворки по управлению программами и портфелями ИТ-проектов Методы мониторинга и контроля управления программами и портфелями ИТ-проектов Методы непрерывного улучшения управления программами и портфелями ИТ-проектов	Осуществлять руководство управлением программами и портфелями ИТ-проектов Формировать команду и организовывать персонал и стейкхолдеров для управления программами и портфелями ИТ-проектов Осуществлять мониторинг и контроль управления программами и портфелями ИТ-проектов Организовывать деятельность по непрерывному улучшению управления программами и портфелями ИТ-проектов
	Способность разработки архитектуры системы защиты информации автоматизированной системы (ПСК-3)	Формирование и согласование принципов управления ценностью ИТ для бизнеса (организации) и инвестициями в цифровую трансформацию Организация управления	Международные и отечественные стандарты, лучшие практики и фреймворки по управлению ценностью ИТ для бизнеса (организации) и инвестициями в цифровую трансформацию	Формировать принципы управления ценностью ИТ для бизнеса (организации) и инвестициями в цифровую трансформацию Формировать команду и организовывать

		ценностью ИТ для бизнеса (организации) и инвестициями в цифровую трансформацию с помощью персонала и стейкхолдеров Контроль инвестиций в цифровую трансформацию	Методы контроля и оценки эффективности инвестиций в цифровую трансформацию	персонал и стейкхолдеров для управления ценностью ИТ для бизнеса (организации) и инвестициями в цифровую трансформацию Осуществлять мониторинг и контроль инвестиций в цифровую трансформацию
	Способность моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации (ПСК-4)	Формирование и согласование потребностей бизнеса (организации, региона, страны) в цифровых технологиях	Международные и отечественные стандарты, лучшие практики и фреймворки по обеспечению динамичного изменения организации (региона, страны) с использованием цифровых технологий	Выявлять потребности бизнеса (организации, региона, страны) в цифровых технологиях Формировать команду и организовывать персонал и стейкхолдеров для обеспечения динамичного изменения организации (региона, страны) с использованием цифровых технологий Осуществлять мониторинг и контроль обеспечения динамичного изменения организации (региона, страны) с использованием цифровых технологий

ПСК-1 - трудовая функция D/01.7 профессионального стандарта «Специалист по защите информации в автоматизированных системах», (утв. Приказом Минтруда России от 19 сентября 2022 № 522н).
ПСК-2 - трудовая функция D/02.7 профессионального стандарта «Специалист по защите информации в автоматизированных системах», (утв. Приказом Минтруда России от 19 сентября 2022 № 522н).
ПСК-3 - трудовая функция D/03.7 профессионального стандарта «Специалист по защите информации в автоматизированных системах», (утв. Приказом Минтруда России от 19 сентября 2022 № 522н).
ПСК-4 - трудовая функция D/04.7 профессионального стандарта «Специалист по защите информации в автоматизированных системах», (утв. Приказом Минтруда России от 19 сентября 2022 № 522н).
ОПК-3- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.04.02 Менеджмент (уровень магистратуры) (утв. Приказом Министерства образования и науки РФ от 12 августа 2020 г. N 92)

1.4. Категория слушателей

Руководители высшего и среднего звена в области информационной безопасности, подразделений по защите информации, информационных технологий, сотрудники частных компаний и государственных организаций, которым требуется повышение

профессионального уровня в области информационной безопасности в соответствии с актуальными изменениями в вопросах защиты информации, имеющие высшее техническое образование (бакалавр, дипломированный специалист, магистр) по специальности связанной с вычислительной техникой, информатикой или информационной безопасностью.

Желательно знание структуры одной из операционных и сетевых сред, умение работать с современными программными средствами.

Имеющие опыт работы не менее одного года в области защиты информации.

1.5. Формы и технологии обучения

Очно-заочная форма обучения. Занятия проводятся с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ). Общая трудоемкость программы 314 академических часа (включая 38 часов с ЭО и ДОТ и 10 часов на итоговую аттестацию), в том числе 100 часов контактной работы со слушателем и 188 академических часов на самостоятельную работу слушателя. Итоговая аттестация проводится в форме итогового экзамена и не требует создание итоговой аттестационной комиссии, проводится одним из преподавателей реализующих данную программу.

1.6. Период обучения, срок освоения и режим занятий

Вечерний формат обучения: срок обучения - 13 недель, режим занятий – два-три вечера в неделю с 19.00 до 22.00 и суббота с 09.00 до 17.00; модульный формат обучения – 5 недель и 5 дней (очный модуль 10 дней), дистанционные занятия по субботам, режим занятий - с 09.00 до 17.00.

1.7. Документ о квалификации

Удостоверение о повышении квалификации Российской академии народного хозяйства и государственной службы при Президенте Российской федерации.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Календарный учебный график

Таблица 2

Календарный учебный график

Вечерний формат обучения						
1 неделя	2 неделя	3 неделя	4 неделя	5 неделя	6 неделя	7 неделя
УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА
8 неделя	9 неделя	10 неделя	11 неделя	12 неделя	13 неделя	
УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	ИА с ДОТ	
Модульный формат обучения						
1 неделя	2 неделя	3 неделя	4 неделя	5 неделя	5 недель, 5 дней	
УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	УЗ ЭО и ДОТ, ТКУ, ПА	ИА с ДОТ	

УЗ ЭО и ДОТ – учебные занятия с применением электронного обучения и дистанционных образовательных технологий
ТКУ – текущий контроль успеваемости
ПА – промежуточная аттестация
ИА ДОТ - итоговая аттестация с применением дистанционных образовательных технологий

2.1. Учебный план

Таблица 3

Учебный план

№п/п	Наименование раздела, модуля, дисциплины, темы, практики, стажировки[2]	Общая трудоемкость, час.	Контактная работа, час.					Самостоятельная работа, час	Контактная работа (с применением дистанционных образовательных технологий), час.[6]					Самостоятельная работа (в т.ч. электронное обучение (ЭО), час	Текущий контроль успеваемости	Промежуточная аттестация (форма/час)[9]	Итоговая аттестация (вид /час.)	Код компетенции
			Всего	В том числе					Всего	В том числе								
				Лекции / в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации			Лекции/ в интерактивной форме	Практические (семинарские/лабораторные) занятия /в интерактивной форме	Контактная самостоятельная работа, час	Индивидуальные и групповые консультации					
1.	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
4.1.	Формирование и реализация политики информационной безопасности	40	16	8/4	8/8			20								Э (Т/4)		**ПСК-2**
4.2.	Стандарты и аудит информационной безопасности ISO 27001	40	16	4/2	12/12			22								ЗО (Т/2)		**ПСК-1**
4.3.	Организация защиты персональных данных и связанные с этим мероприятия	48	12	4/2	8/8			34								ЗО (Т/2)		**ПСК-3**
4.4.	Защита критической информационной инфраструктуры	40							12	4/2	8/8			26		З (Д/2)		**ПСК-3**
4.5.	Эффективность защиты информации	56	16	8/4	8/8			38								ЗО (Т/2)		**ПСК-3**
4.6.	Законодательство информационной безопасности	40	12	4/2	8/8			26								З (Т/2)		**ПСК-2**
4.7.	Комплексное обеспечение информационной безопасности в интернет	40	16	8/4	8/8			22								ЗО (2)		**ПСК-3**
	Итого:	304	88	36	52			162	12	4	8			26		**16**		
	Итоговая аттестация	10						6									Экзамен (Т/4)	
	Всего:	**314**	**88**	36	52			**168**	**12**	4	8			**26**		**16**	**4**	

2.2. Содержание программы по дисциплинам

Таблица 4

Содержание программы по дисциплинам

Номер дисциплины	Содержание дисциплины
1. *Формирование и реализация политики информационной безопасности*	*Нормативно-правовые основы информационной безопасности. Политика обеспечения информационной безопасности. Функции обеспечения информационной безопасности и инструменты их реализации. Связь информационной безопасности, вопросов планирования непрерывности бизнеса и задач анализа информационных процессов и потоков.* *Формализация системного подхода к обеспечению информационной безопасности. Сформировать интегрированную систему взглядов на цели, задачи, основные принципы и направления деятельности в области в области обеспечения ИБ с учетом действующего законодательства РФ, а так же Международных стандартов.*
2. *Практика применения требований ISO 27001. Банковские стандарты*	*Понятие Международного стандарта в области информационной безопасности ISO 27001. Определение требований для разработки, реализации, мониторинга, эксплуатации и совершенствования документированной системы управления информационной безопасностью (СУИБ).*
3. *Организация защиты перс. данных и связанные с этим мероприятия*	*Противоречия и неурегулированные вопросы использования и обработки персональных данных. Применение отраслевых стандартов при реализации требований федерального законодательства в сфере персональных данных.* *Создание системы защиты персональных данных.*
4. *Защита критической информационной инфраструктуры*	*Кратко о КИИ. Основные понятия КИИ.* *Категорирование. Процедура категорирования* *приказами ФСТЭК)* *КИИ – это не разовый Проект* *Три кольца процессов*
5. *Внутренние угрозы информационной безопасности*	*Теория внутренней информационной безопасности: постановка задачи, модель угроз, классификация нарушителей. Типы нарушителей, манипуляции и противодействие манипуляциям.* *Построение проекта защиты от внутренних угроз: определение целей, выбор методов, определение критериев успешности.* *Технические средства защиты от внутренних угроз, оценка их достоинств и недостатков, определение их места в системе информационной безопасности.* *Технологии, применяемые в продуктах, используемых для защиты от внутренних угроз*
6. *Законодательство информационной безопасности*	*Понятие и структура информационной безопасности* *Российское законодательство в области информационной безопасности* *Уровни мер по защите интересов субъектов информационных* *Группы мер на законодательном уровне*
7. *Комплексное обеспечение информационной безопасности в интернет*	*Интернет – необходимый элемент работы организации. Интернет как источник большого числа угроз информационной безопасности. Решения по защищенному доступу к сети интернет: защита от компьютерных вирусов и другого вредоносного программного обеспечения, которое может проникнуть в локальную сеть*

	организации из интернета; защита от внешних сетевых атак, направленных на информационные ресурсы компании; мониторинг и аудит доступа пользователей к сети интернет. *Проектирование и внедрение комплексных систем защиты автоматизированных систем. Защита системы в целом и отдельных ее компонент: интернет – портал; внутренний интернет – портал; система электронного документооборота; почтовая система; ERP – система; корпоративная локальная сеть; автоматизированная банковская система и др.*

3. ОРГАНИЗАЦИОННЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое и программное обеспечение реализации программы

Для проведения занятий и итоговой аттестации необходимо материально-техническое обеспечение учебных аудиторий (наглядными материалами, экраном, мультимедийным проектором с ноутбуками (ПК) для презентации учебного материала, выходом в сеть Интернет, лицензионными программными продуктами Microsoft Office (Excel, Word, PowerPoint)) в зависимости от типа занятий: семинарского и лекционного типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для проведения занятий различного типа с использованием электронного обучения и дистанционных образовательных технологий используется учебный образовательный портал на базе Moodle для размещения учебных материалов и интегрированная с ним система BigBlueButton для проведения занятий в формате видео-конференций.

Преподавателям и слушателям необходимо помещение для занятий, оснащенное компьютером с выходом в сеть Интернет, лицензионными программными продуктами Microsoft Office (Excel, Word, PowerPoint), доступ в электронную информационно-образовательную среду организации и ЭБС.

3.2. Учебно-методическое и информационное обеспечение программы

Все методические материалы, презентации, описание кейсов, все необходимые нормативно-правовые документы выкладываются в электронном виде на учебный портал в систему Moodle, где также проходят тестирования, дистанционные консультации преподавателей и сдача кейсов и курсовых работ.

У слушателей, как и у всех студентов Академии, имеется доступ к научной библиотеке Академии, насчитывающей более 1 000 000 экземпляров книг по всем областям знаний. В Академии организован доступ к следующим информационным ресурсам: ЭБС IPRBOOKS, ЭБС ЮРАЙТ, ЭБС ИЗДАТЕЛЬСТВА "ЛАНЬ" в том числе Англоязычные информационные ресурсы: Bloomberg, EBSCO Publishing, Emerging Markets Information Service, IMF eLibrary, JSTOR, New Palgrave Dictionary of Economics, SCOPUS, SCIENCE DIRECT, Web of Science, Wiley Online Library, World Bank Elibrary, OXFORD HANDBOOKS ONLIN, PASSPORT EUROMONITOR INTERNATIONAL, OECD ILIBRARY; и Русскоязычные информационные ресурсы: eLIBRARY.RU, Google Scholar (Google Академия), Polpred.com Обзор СМИ, СИСТЕМА ПРОФЕССИОНАЛЬНОГО

АНАЛИЗА РЫНКОВ И КОМПАНИЙ «СПАРК», ЭЛЕКТРОННАЯ БИБЛИОТЕКА ИЗДАТЕЛЬСКОГО ДОМА «ГРЕБЕННИКОВ».

Самостоятельная работа.

Слушатели самостоятельно изучают материалы, расположенные на образовательной платформе https://ls.itmane.ru.

Примерные темы для самостоятельной работы.

1. Антивирусная защита
2. Безопасность компьютерных систем. традиционный подход к анализу проблем информационной безопасности
3. Выбор мер защиты информации для их реализации в информационной системе в рамках системы защиты информации
4. Доступность информации
5. Законодательный уровень информационной безопасности
6. Защита информационной системы, ее средств и систем связи и передачи данных
7. Защита машинных носителей информации
8. Защита среды виртуализации
9. Защита технических средств
10. информационной безопасности
11. Контроль (анализ) защищенности информации
12. Обнаружение (предотвращение) вторжений
13. Объектно-ориентированный подход – перспективный принцип анализа вопросов
14. Ограничение программной среды
15. Основные определения и критерии классификации угроз
16. Регистрация событий безопасности
17. Управление доступом субъектов доступа к объектам доступа
18. Целостность информационной системы и информации

Подготовка к практическим занятиям.

Подготовка к практическим занятия по дисциплинам учебной программы основана на изучении учебных материалов, размещенных на образовательной платформе https:// ls.itmane.ru.

Примерные задания для проведения практического занятия.

Вопрос 1.
Что относится к правовым методам, обеспечивающим информационную безопасность:
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Вопрос 2.
Что является основными источниками угроз информационной безопасности:
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы

Вопрос 3.
Какие виды информационной безопасности Вы знаете:
- Клиентская, серверная, сетевая
- Персональная, корпоративная, государственная
- Локальная, глобальная, смешанная

Вопрос 4.
Цели информационной безопасности – своевременное обнаружение, предупреждение:

- инсайдерства в организации
- несанкционированного доступа, воздействия в сети
- чрезвычайных ситуаций

Вопрос 5.

Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

Нормативно-правовые документы.

1. Конституция РФ (ст. 15 п.4, ст.44, ст. 71 п. «о»).
2. Гражданский Кодекс РФ с изменениями и дополнениями от 12 марта 2014г.№35-ФЗ.
3. Гражданский процессуальный кодекс РФ.
4. Налоговый кодекс РФ часть I, часть II с изменениями и дополнениями.
5. Таможенный кодекс РФ.
6. Уголовный кодекс РФ.
7. Закон РСФР от 22.03.1991г. № 948 «О конкуренции и ограничении монополистической деятельности на товарных рынках» (в ред. от 26.07.2006 г. № 135-ФЗ).
8. Закон РФ «О залоге» от 20.05.1992 г. № 2872-1 (в ред. от 19.07.2007 г. № 197-ФЗ).
9. Федеральный закон «О науке и государственной научно-технической политике» от 23.08.1996 г. № 127-ФЗ с изменениями и дополнениями.
10. Федеральный закон РФ от 29.07.2004г. № 98-ФЗ «О коммерческой тайне».
11. Федеральный закон РФ «О защите конкуренции» от 26.07.2006г. № 135-ФЗ (в ред. 30.06.2008 г. № 108-ФЗ).
12. Федеральный закон Российской Федерации от 27.06.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
13. Федеральный Закон РФ от 27.07.2006 г. № 157-ФЗ «О внесении изменений в федеральный закон «Об оценочной деятельности в РФ» (в ред. от 13.07.2007 № 129-ФЗ).
14. Положение по бухгалтерскому учету «Учет расходов на научно-исследовательские, опытно-конструкторские и технологические работы» ПБУ 17/02. Приказ Минфина РФ от 19.11.2002 г. № 115н.
15. «Методические рекомендации по определению рыночной стоимости интеллектуальной собственности» утверждены Министерством имущественных отношений РФ 26.11.2002 г. № СК-4/21297.
16. Приказ Государственного таможенного комитета Российской Федерации от 27.10.2003г. № 1199 «Об утверждении Положения о защите прав интеллектуальной собственности таможенными органами».
17. «Методические рекомендации для руководителей предприятий по вопросам учета, правовой охраны и использования результатов научно-технической деятельности, созданных за счет средств федерального бюджета» утв. министром образования и науки РФ А.А. Фурсенко 26.07.2004 г.
18. Положение по бухгалтерскому учету «Учет нематериальных активов» ПБУ 14/2007. Приказ Минфина от 27.12.2007 г. № 153н.
19. Постановление Правительства РФ от 24.12.2007 г. № 928 «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение и полезную модель, созданных в РФ, сведений, составляющих государственную тайну».
20. Постановление Правительства РФ от 15.09.2008г. №691 «Об утверждении Положения о лицензировании внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), в отношении которых установлен экспортный контроль».
21. Постановление Правительства РФ от 24 декабря 2008 г. № 1020 об утверждении «Правил государственной регистрации договоров о распоряжении исключительным правом».

22. Федеральный закон Российской Федерации от 25 декабря 2008 г. № 284-ФЗ «О передаче прав на единые технологии».
23. Постановление Правительства РФ от 25.02.2011 г. №107 «О порядке применения в РФ стандартов МФСО».
24. Указ Президента РФ от 24 мая 2011 г. № 673 «О Федеральной службе по интеллектуальной собственности».
25. Федеральный закон Российской Федерации от 8 декабря 2011 г. № 422-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с созданием в системе арбитражных судов Суда по интеллектуальным правам».
26. Распоряжение Правительства РФ от 8 декабря 2011 г. № 2227-р «О Стратегии инновационного развития РФ на период до 2020 г.»
27. Приказ Министерства Обороны Российской Федерации от 23 июля 2012 г. №2020 «Об утверждении Административного регламента предоставления Министерством обороны Российской Федерации государственной услуги по организации рассмотрения заявок и выдачи патентов на секретные изобретения, относящиеся к средствам вооружения и военной техники».
28. Постановление Правительства РФ №458 от 30 мая 2013 г. «О внесении изменений в правила осуществления государственными заказчиками управление правами Российской Федерации на результаты интеллектуальной деятельности гражданского, военного, специального и двойного назначения».
29. Постановление Правительства Российской Федерации от 12 апреля 2013 г. №327 г.Москва «О единой государственной информационной системе учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения».
30. Федеральный закон от 2 июля 2013 года № 187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».(Антипиратский закон)
31. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
32. Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности"
33. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи"
34. Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании"
35. Федеральный закон от 07.07.2003 N 126-ФЗ "О связи"
36. Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"
37. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"
38. Приказы и руководящие документы ФСТЭК России, ФСБ России и Роскомнадзора по защите конфиденциальной информации и персональных данных
39. Федеральный закон РФ от 1 марта 2020г. № 33-ФЗ «О внесении изменений в Федеральный закон «О защите конкуренции».
40. Распоряжение Правительства РФ от 03 августа 2020г. № 2027-р « Об утверждении плана мероприятий («дорожной карты») по реализации механизма управления системными изменениями нормативно-правового регулирования предпринимательской деятельности «трансформация делового климата в сфере интеллектуальной собственности».
41. Федеральный закон от 08 декабря 2020г. № 399-ФЗ « О внесении изменений в ст.5 Федерального Закона « О науке и государственной научно-технической политике» и ст.103 Федерального Закона « Об образовании в Российской Федерации».
42. Федеральный закон РФ от 21 декабря 2021 г. № 416 –ФЗ « О внесении изменений в Федеральный закон « О патентных поверенных»
43. Федеральный закон РФ о 7 октября 2022г. №386-ФЗ «О внесении изменения в ст.1363 части четвертой Гражданского кодекса Российской Федерации»

44. Указ Президента РФ от 30.03.2022 N 166 (ред. от 22.11.2023) "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации"
45. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025г.)
46. Федеральный закон от 23.07.2025 N 255-ФЗ "О внесении изменений в Федеральный закон "О федеральной информационной адресной системе и о внесении изменений в Федеральный закон "Об общих принципах организации местного самоуправления в Российской Федерации"
47. Распоряжение Правительства РФ от 12.07.2025 N 1880-р "Об определении организации обеспечивающей создание и функционирование многофункционального сервиса обмена информацией"
48. Распоряжение Правительства РФ от 05.07.2025 N 1805-р "Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования до 2030 года и признании утратившим силу распоряжения Правительства РФ от 21.12.2021 N 3759-р"
49. Постановление Правительства РФ от 30.06.2025 N 981 "О государственной информационной системе удаленного использования архивных документов и справочно-поисковых средств к ним" (вместе с "Положением о государственной информационной системе удаленного использования архивных документов и справочно-поисковых средств к ним")
50. Постановление Правительства РФ от 22.05.2025 N 702 "Об утверждении Правил проверки соответствия пользователей государственной информационной системы, определенной в соответствии с частью 2 статьи 13.1 Федерального закона "О персональных данных", требованиям, указанным в части 7 статьи 13.1 Федерального закона "О персональных данных"
51. Постановление Правительства РФ от 17.01.2023 N 30 "О стандартах раскрытия информации субъектами естественных монополий, осуществляющими деятельность в области оказания услуг связи"

Основная литература

1. Рабчевский, А. Н. Синтетические данные и развитие нейросетевых технологий : учебное пособие для вузов / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2023. — 187 с.
2. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для вузов / Л. А. Станкевич. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 495 с.
3. Платонов, А. В. Машинное обучение : учебное пособие для вузов / А. В. Платонов. — Москва : Издательство Юрайт, 2023. — 85 с.
4. Загорулько, Ю. А. Искусственный интеллект. Инженерия знаний : учебное пособие для вузов / Ю. А. Загорулько, Г. Б. Загорулько. — Москва : Издательство Юрайт, 2022. — 93 с.
5. Бессмертный, И. А. Интеллектуальные системы : учебник и практикум для вузов / И. А. Бессмертный, А. Б. Нугуманова, А. В. Платонов. — Москва : Издательство Юрайт, 2023. — 243 с.
6. Информационные технологии в менеджменте : учебник для вузов / под редакцией Е. В. Майоровой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 303 с. — (Высшее образование). — ISBN 978-5-534-20286-1. — Текст : электронный // Образовательная платформа Юрайт [сайт].

7. Малюк, В. И. Стратегический менеджмент. Организация стратегического развития : учебник и практикум для вузов / В. И. Малюк. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 404 с. — (Высшее образование). — ISBN 978-5-534-17159-4. — Текст : электронный // Образовательная платформа Юрайт [сайт].
8. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590420 (дата обращения: 04.02.2026).
9. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590419 (дата обращения: 04.02.2026).

Дополнительная литература

1. Белов Е.Б. Основы защиты информации. М.: Изд. «Горячая линия – Телеком», 2006.
2. Коняев И., Беляев А. Информационная безопасность предприятия. – СПб.: «БХВ-Петербург», 2003
3. Котухов М.М. Цикл лекций по курсу «Комплексное обеспечение информационной безопасности автоматизированных систем». Учебное пособие. Лекции 1 – 6. – М.: Изд. АНХ, 2012. – 346 с., (электронный вариант).
4. Разработка систем информационно-компьютерной безопасности /В.М.Зима, М.М.Котухов, А.Г.Ломако, А.С.Марков, А.А.Молдовян. - СПб.: «Наука и техника», 2013. – 327 с., (электронный вариант).
5. Толстобров, А. П. Архитектура ЭВМ : учебник для вузов / А. П. Толстобров. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 222 с. — (Высшее образование). — ISBN 978-5-534-21569-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583536 (дата обращения: 04.02.2026).
6. Долганова, О. И. Моделирование бизнес-процессов : учебник и практикум для вузов / О. И. Долганова, Е. В. Виноградова, А. М. Лобанова ; под редакцией О. И. Долгановой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-534-17914-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583398 (дата обращения: 04.02.2026).

Интернет-ресурсы и справочные системы

1. Никольская Ю.П. Мерзликина Е.М. аудит учебное пособие http://hi-edu.ru/e-books/xbook086/01/part-002.htm#i33
2. Е. Царев Исследование «Рынок информационной безопасности Российской Федерации» http://www.tsarev.biz/informacionnaya-bezopasnost/zakonchilsya-proekt-pervogo-ekspertnogo-issledovaniya-rossijskogo-rynka-ib/
3. Предпринимательское право http://businesspravo.ru/
4. Информационный канал Государственной Думы http://www.akdi.ru/gd/akdi.htm
5. Система Гарант http://www.garant.ru/
6. Консультант Плюс http://www.consultant.ru/
7. ОАО «ИнфоТеКС» http://www.infotecs.ru/gtc
8. Российский сервер по безопасности http://www.secur.ru
9. Весь Рынок Безопасности России - Sec.Ru http://www.sec.ru/
10. Журнал «Защита информации. Конфидент» http://www.confident.ru/magazine
11. «БДИ» (Безопасность, Достоверность, Информация) : http://www.bdi.spb.ru/

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Промежуточная аттестация по каждому курсу выступает в форме зачета или экзамена. В зависимости от поставленных задач курса зачет или экзамен может быть представлен в виде кейса, теста, деловой игры или задания.

Тема 1.1. Формирование и реализация политики информационной безопасности
Промежуточная аттестация по теме «Формирование и реализация политики информационной безопасности» осуществляется в виде экзамена, который включает в себя задание.

Оценка «отлично» выставляется, если ответы соответствуют теме задания, заданному объему, полноте и обоснованности решения, полученные результаты соответствуют поставленной цели, слаженная командная работа.

Оценки «хорошо» выставляется, если ответы соответствуют теме задания, заданному объему, полноте и обоснованности решения, результаты соответствуют поставленной цели, не слаженная командная работа.

Оценки «удовлетворительно» выставляется, если ответы соответствуют теме задания, соблюдены требования к объему, нет обоснованности решения, полученные результаты не в полной мере соответствуют поставленной цели.

Оценка «неудовлетворительно» выставляется, если ответы не соответствуют теме задания, заданному объему, решение не обоснованно, полученные результаты не соответствуют поставленной цели.

Примерное задание по курсу Формирование и реализация политики информационной безопасности:
Произвести аудит комплексной безопасности предприятия.
Состав блоков вопросов программы:
М 1. Оценивания показателя обеспечения безопасности при назначении и распределении ролей и обеспечении доверия к персоналу.
М 2. Оценивания показателя обеспечения безопасности коммерческих информационных технологических процессов.
М 3. Оценка показателя обеспечения информационной безопасности при определении/уточнении области действия процессов управления безопасностью бизнеса.
М 4. Оценка показателя обеспечения безопасности при оценке рисков безопасности бизнеса, вариантов минимизации рисков безопасности бизнеса.
М 5. Оценки показателя обеспечения безопасности при определении/уточнении политики безопасности бизнеса хозяйствующего объекта.
М 6. Оценка показателя обеспечения безопасности при выборе/уточнении целей безопасности бизнеса и защитных мер.
М 7. Оценки показателя обеспечения безопасности при принятии руководством хозяйствующего объекта решения о реализации, эксплуатации и совершенствовании процессов управления безопасностью бизнеса.
М 8. Оценки показателя обеспечения безопасности при определении плана минимизации рисков безопасности бизнеса.
М 9. Оценки показателя обеспечения информационной безопасности при реализации защитных мер, управления работами и ресурсами.
М 10. Оценки показателя обеспечения безопасности при реализации программы по обучению безопасности бизнеса.
М 11. Оценки показателя обеспечения безопасности при обнаружении и реагировании на инциденты безопасности бизнеса.
М 12. Оценки показателя обеспечения информационной безопасности (ИБ) при анализе качества процессов управления безопасностью бизнеса.
М 13. Оценки показателя обеспечения безопасности при аудите хозяйствующего объекта

Тема 1.2. Стандарты и аудит информационной безопасности ISO 27001

Промежуточная аттестация по теме «Стандарты и аудит информационной безопасности ISO 27001» осуществляется в виде зачета с оценкой, который включает в себя прохождение тестирования.

Оценка «отлично» выставляется, если дано от 81% до 100% правильных ответов

Оценки «хорошо» выставляется, если дано от 65% до 80% правильных ответов

Оценки «удовлетворительно» выставляется, если дано от 50% до 64% правильных ответов

Оценка «неудовлетворительно» выставляется, если дано менее 50% правильных ответов.

Примерные вопросы теста:

Раздел 1

1) Что из следующего подтверждает «адекватность», которую ищет аудитор?
   a) Адекватно ли объяснена система персоналу?
   b) Способна ли компания достичь своих целей, действуя в соответствии со стандартом/положениями ВНД?
   c) Соответствует ли документация требованиям стандарта/положениям ВНД и способствует ли такая документация выполнению целей компании?
   d) Все из выше перечисленного.
   e) Ничего из вышеперечисленного.
2) Укажите правильную последовательность проведения аудита:
   a) Планирование – подготовка-проведение аудита-составление отчета-последующая проверка и закрытие несоответствий.
   b) Планирование- проведение аудита- подготовка- составление отчета-последующая проверка и закрытие несоответствий.
   c) Подготовка-планирование-проведение аудита- составление отчета-последующая проверка и закрытие несоответствий.
   d) Подготовка –проведение аудита-составление отчета-планирование-последующая проверка и закрытие несоответствий
3) Что должно сделать подразделение, подвергшееся аудиту, после аудита?
   a) Если нет несоответствий, ничего не делать, просто улучшать систему
   b) Провести расследование причин несоответствий
   c) Выбрать корректирующие действия, провести их и предотвратить повторение несоответствий.
   d) a и c
   e) все из выше перечисленного
4) Что из ниже перечисленного не является задачей аудиторов?
   a) Проводить аудиты
   b) Составлять письменные отчеты по аудиту
   c) Составлять опросные листы
   d) Составлять планы аудитов
   e) Составлять письменный запрос на корректирующие действия
5) Что не должно быть написано в отчете?
   a) Наблюдения
   b) Соответствия пунктастандарта/положений ВНД
   c) Обнаруженные несоответствия
   d) Информация, содержащая коммерческую тайну, полученная от подразделения, проходящего аудит
   e) Список аудиторов

Раздел 2

1. Чтобы вы спросили? Чтобы проверить п.4.2.1 Стандарта? (не меньше 5 вопросов)
2. Напишите 5 документов которые должны быть в организации? В соответствии с требованиями ISO 270001
3. Перечислите шесть личных качеств , необходимых для аудитора

4. Выберите две меры контроля из Приложения А, которые внедрены в нашей Организации, и объясните, как они применяются.

Раздел 3

Во время аудита были обнаружены несоответствия. Пожалуйста, заполните форму запроса на корректирующее действие.

1. Аудитор Александр 20 января 2014 года во время проведения аудита по ВНА «Политика безопасности для компьютерных пользователей» отдела обработки заказов обнаружил, что компьютерное оборудование установлено на подоконниках и не подключено. В беседе с сотрудниками выяснилось, что они первый день как переехали после произведенного ремонта и еще не успели подключить оборудование, так как грузчики только что установили столы. На вопрос аудитора, проинформировали ли они ИТ подразделение о переезде, сотрудник ответил, что он и сам не плохо разбирается в компьютерах и никакой необходимости в дополнительной помощи у него нет.

Форма запроса на корректирующее действие
Проверяемое подразделение Аудиторы №запроса Дата аудита
Описание несоответствия:

2. Аудитор Наталья при проведении аудита по ВНА «Политика безопасности для компьютерных пользователей» энергетической службы 15.03.2014 увидела на мониторе сотрудника три листка для заметок разного цвета со словами логин и пароль. В беседе сотрудник сказал, что листочки разного цвета сделаны для удобства, когда в его отсутствие кому-то из коллег нужно срочно сделать что-то в информационных системах, то они не теряют времени на поиск пароля. Индивидуальных паролей у них нет, так как они следят за затратами и таким образом экономят деньги на лицензиях.

Форма запроса на корректирующее действие
Проверяемое подразделение Аудиторы №запроса Дата аудита
Описание несоответствия:

Раздел 4

1) Во время аудита были обнаружены следующие ситуации. Пожалуйста, напишите, какие пункты Стандарта/положений ВНД применимы в этих случаях.
2) Люди, не имеющие разрешения находиться на территории, без сопровождения зашли в комнату, в которой находятся крайне важные активы……
……
3) Из-за недостатка ресурсов организация отложила установку пожаропрочных дверей и новых систем обнаружения и тушения пожара, и поэтому действия, упомянутые в плане обработки риска , не выполняются
4) ……
……
5) Организация не вносит в договора, предусматривающими доступ к конфиденциальной информации и коммерческой тайне компании раздел о конфиденциальности и неразглашении……
……
6) Аудитор делает пометки о номерах редакций процедур в отделе кадров. В отделе ИТ используются другие редакции тех же

документов……
……

7) Аудитор увидел, что несмотря на большое количество изменений, отчет по оценке риска не обновлялся уже два года
……
……

Из десяти опрошенных во время аудита сотрудников, пятеро никогда не слышали о политике ИБ
……
……

За тест максимально можно получить 100 баллов. Зачет выставляется при наборе более 70 баллов.

Максимальный балл за раздел: Раздел 1: 20 баллов (4 балла за каждый вопрос)
Раздел 2: 30 баллов (7,5 баллов за каждый вопрос)
Раздел 3: 20 баллов(10 баллов за каждый вопрос)
Раздел 4 30 баллов (5 баллов за каждый вопрос)

Тема 1.3. Организация защиты персональных данных и связанные с этим мероприятия

Промежуточная аттестация по теме «Организация защиты персональных данных и связанные с этим мероприятия» осуществляется в виде зачета с оценкой, который включает в себя ответы на вопросы.

Оценка «отлично» выставляется, если слушатель показал глубокое полное знание и усвоение материала учебной темы, его взаимосвязи с другими темами и с предстоящей профессиональной деятельностью, усвоение основной литературы, и знание дополнительной литературы, способность к самостоятельному пополнению и обновлению знаний.

Оценки «хорошо» заслуживает слушатель, показавший полное знание основного материала учебной темы, знание основной литературы и знакомство с дополнительной литературой, способность к пополнению и обновлению знаний.

Оценки «удовлетворительно» заслуживает слушатель, показавший при ответе на экзамене знание основных положений учебной темы, допустивший отдельные погрешности и сумевший устранить их с помощью экзаменатора, знакомый с основной литературой.

Оценка «неудовлетворительно» выставляется, если при ответе выявились существенные пробелы в знаниях слушателя основных положений учебной темы, неумение даже с помощью экзаменатора сформулировать правильные ответы на вопросы.

Примерные вопросы:

Вопросы 1

1. Необходимо ли привлечение подрядчика с лицензией для ввода в эксплуатацию СКЗИ для ИСПДн К3 или достаточно закупить сертифицированные СКЗИ и устанавливать его своими силами?
2. Возможно ли осуществить все мероприятия по защите персональных данных без нарушения законодательства своими силами, с учетом того, что персональные данные будут классифицированы как К3?
3. С учетом рекомендаций Роскомнадзора по осуществлению проверок в документарной форме, правильно ли делать в первую очередь разработку и внедрение ОРД и журналирование деятельности для закрытия формальных требований по защите?
4. Проходили ли успешную проверку НПФ, взявшие за основу СТО НАПФ?

Насколько корректным будет использования Р НАПФ 4.3 2010 Рекомендации по формированию ОРД для коммерческой организации, с учетом собственной специфики?

5. При осуществлении деятельности требуется передача персональных данных в ПФ, ФСС, банки, страховые компании и т.п. Имеются требования, чтобы субъект давал согласие на передачу своих персональных данных конкретным операторам по обработке персональных данных. Каким образом лучше организовать процедуру принятия (изменения) конкретного списка операторов?
6. Какие реальные последствия возможны в случае выявления нарушений по защите персональных данных, если они обрабатываются в рамках Трудового законодательства.
7. Сколько по срокам должны храниться: журнал обращений субъектов ПДн, журнал регистрации о выдаче копий документов, журнал передачи ПДн третьей стороне, журнал регистрации электронных носителей?
8. Можно ли объявить всю филиальную сеть единой ИСПДн, с необходимостью защиты центра, каналов связи и филиалов с выполнением всех обязательных требований по защите персональных данных одновременно ко всем элементам?

Вопросы 2

1. 25 января 2012 Европейская комиссия официально выпустила свое предложение по реформе правил защиты данных 1995 года об обработке персональных данных. Предлагаемое положение было опубликовано на веб-сайте Европейской комиссии. Влияет ли данный факт каким-то образом на требования по защите ПДн на территории РФ? Имеет ли отношение к данному обстоятельству намерение Совета Федерации создать независимый орган для защиты персональных данных физлиц?
2. Являются ли обязательными ведомственные требования ФСТЭК в области сертификации СЗИ (в т.ч. определенные ФСТЭК, ФЗ-184, ст.5) для защиты сведений, не составляющих государственную тайну?
3. В связи с тем, что ФСТЭК России опубликовал на своем сайте документы, касающиеся требований к системам обнаружения вторжений в ИСПДн 1, 2, 3, 4 http://www.ispdn.ru/news/9466/ нужно ли применять какие-либо дополнительные мероприятия в случае, если система обнаружения атак реализована с помощью CheckPoint Firewall NG?
4. На сайте РКН публикуются перечни ресурсов, закрытых за распространение ПД. Например http://www.rsoc.ru/docstore/doc1124.htm?print=1, http://www.rsoc.ru/docstore/doc1125.htm?print=1. На каком основании и как осуществляется данное блокирование? Какова сфера блокирования доменов .com?
5. Нарушает ли владелец сайта закон, если на его сайте кто-то опубликовал данные о человеке без его согласия? Например, законодательство для некоторых видов деятельности обязывает публиковать сведения о лицах (группах лиц), оказывающих существенное влияние на решения, принимаемые органами управления компанией. Это могут быть и физлица. Должно ли в данном случае присутствовать документально оформленное согласие от этих физлиц?
6. Можно ли, в принципе, размещать информационные системы персональных данных (ИСПДн) в «облаке» с учетом требований регулирующих органов по защите информации?
7. Рассмотрим 152-ФЗ в кредитной организации, не присоединившейся к СТО БР. Можно ли, организационно запретив администраторам ИС ознакамливаться с ПДн, обрабатываемых в ИС, исключить необходимость построения систем технической защиты при условии, что вся остальная обработка проводится лицами с финансовым и банковским профильным образованием, чьи действия попадают под необходимость сохранения банковской тайны?
8.ИСПДн брокерского обслуживания на финансовых рынках класса К2 - подключение рабочих мест пользователей к серверу осуществляется в терминальном режиме по оборудованию "тонкого клиента". Нужно ли проводить построение технической защиты на рабочих местах (тонких клиентах), если они отделены от терминального сервера (на котором хранятся данные) с помощью МЭ 3-го класса?
9. Компания, имеющая 100%-ную дочку в стране Еврозоны. Осуществляется передача в европейский офис данных, ИСПДн 2/3 категории, обезличивание до 4-й проблематично.. Является ли это передачей персональных данных? А если передавать ID с инициалами?

Вопросы 3

1. Являются ли платежные системы (например SWIFT) - ИСПДн?

В SWIFT - встречается ФИО получателя, его платежные реквизиты, адрес. ИНН получателя побычно не пишут, хотя иногда могут и написать. Случается, что клиенты-физлица указывают ИНН

По мнению ЦБ (цитата отсюда http://forum.npsib.org/viewtopic.php?id=46) - это не ИСПДн, т.к. обработка ПДн не является предназначением системы, а ПДн лишь являются сопутствующей основным целям информацией и выделить обработку ПДн в отдельную обработку не представляется возможным.

А с другой стороны система SWIFT является международной и там работает конвенция + 152-ФЗ. Фактически это ЭДО. (цитата оттуда же)

Как правильно?

2. Достаточно ли для удовлетворения техническим требованиям 152-ФЗ ИСПДн класса К3/К2 при многопользовательском режиме обработки ПД и разных правах доступ к ним пользователей следующих мероприятий, осуществленных средствами операционных систем

а) управление доступом:

идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длинной не менее восьми буквенно-цифровых символов;

б) реализация регистрации и учета :

регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;

в) обеспечение целостности:

обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

плюс

- физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации (средствами ЧОП)
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа (сканер безопасности например XSpider)
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности (контроль состояния эталонных носителей)

3. Нюансы оценки ИСПДн меньшего класса (снижения класса ИСПДн)?

Например, ПК администратора относится к двум сетям:

- 1-ая – сеть услуг брокерского дистанционного обслуживания клиентов (3 класс);
- 2-ая – сеть бухгалтера (2 класс);

Стандартный прием - провести сегментирование (разделение ИСПДн или АС на взаимодействующие участки сети) с помощью межсетевых экранов, поскольку в соответствии с п. 2.4 Приложения к «Положению о методах и способах защиты информации в информационных системах персональных данных» «...При разделении информационной системы при помощи межсетевых экранов на отдельные части для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом...»

Возможны ли другие варианты с меньшими затратами и менее сложной инфраструктурой?

4. Клиенты кредитной организации беспокоятся о потенциальном риске утечки их персональных данных и данных об их финансовых операциях, составляющих банковскую тайну, вследствие ненадлежащей охраны данной информации в РКН. Примеры ненадлежащего хранения ПДн в РКН например здесь http://www.ispdn.ru/news/9564/.

В случае присоединния кредитной организации к СТО БР вправе ли РКН проводить проверку соблюдения требований 152-ФЗ в кредитной организации?

Каковы действия кредитной организации в случае прихода проверки РКН?

5. На контролируемой территории находятся несколько компаний, принадлежащих к одной группе - одна кредитная организация, вторая - инвестиционная компания, профучастник рынка ЦБ. У кредитной организации отраслевой стандарт СТО БР, у инвестиционной компании - профучастника рынка ЦБ - отраслевой станрдарт ФСФР. Как совмещать требования разных отраслевых стандартов для компаний, находящихся на одной контролируемой территории там, где есть нюансы, относящиеся к физической безопасности?

6. Нюансы классификации ИСПДн по СТО БР

п.6 Положения об обеспечении безопасности ПДн в ИСПДн (утверждено Постановлением Правительства № 781) гласит:

Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

Выводы:

1. Классификация в зависимости от объёма и угроз;
2. Порядок классификации устанавливают ФСТЭК, ФСБ, Минсвязи (в структуру которого входит РКН).

Теперь рассмотрим классификацию Банка России, описанную в п.5.2 РС БР ИББС-2.3.2010:

- ИСПДн-С - система обрабатывающая спец. категории ПДн (главным образом сведения о здоровье);
- ИСПДн-Б - система обрабатывающая биометрию (фотографию или скан паспорта с фото, к примеру);
- ИСПДн-Д - система обрабатывающая обезличенные или общедоступные ПДн;
- ИСПДн-И - система обрабатывающая все остальные типы ПДн (тут у нас сидят 99% всех ИСПДн).

Т.к. про объём обрабатываемых ПДн тут не слова нет, а в ПП781 нет ни слова про Банк России,

- может ли кредитная организация игнорировать классификацию по стандарту Банка России, если она официально не присоединяется к СТО БР?
- может ли кредитная организация игнорировать классификацию по ПП 781, если она официально присоединилась к СТО БР?

7. Рассмотрим кредитную организацию, в которой стоит запись телефонных разговоров. Как в этом случае быстро взять согласие на обработку, и т.п.? Или в данном случае и не надо брать согласие на обработку. Кредитная организация должна доказать наличие согласия. И для этого перед началом записи разговора с оператором кредитной организации достаточно использовать робота, который сообщает, что в целях обеспечения защиты ПД и повышения качества обслуживания все переговоры записываются, и после этого абонент вступает с вами в разговор. И данная запись подтвердит , что клиент кредитной организации, продолжающий разговор, совершил конклюдентные действия и, зная о записи переговоров, этими действиями дал согласие их продолжить.
8. Должен ли работодатель получать согласие работника на обработку его ПД по ДМС? С ОМС проще, в связи с принятием нового ФЗ о "Обязательном медицинском страховании" на обработку персональных данных в системе обязательного медицинского страхования согласие брать не нужно. Потому что в 9 статье написано, что законы могут определять случаи обязательного предоставления персональных данных для обеспечения, в частности, защиты здоровья граждан. А как насчет ДМС? И что, если такое согласие уже берет страховая компания - работодатель должен ли брать такое согласие?
9. Согласно разъяснения по медицинской инфе http://tltkrepost.ru/FAQ.html,
Если в БД есть только ФИО и дата рождения + остальные медицинские данные, паспортных данных и адреса прописки нет, можно ли считать такие данные обезличенными и к какому классу такая система относится? Или это вообще не относится к 152 ФЗ?

- Безусловно, относится к 152 ФЗ. Обезличенными считать нельзя, т.к. ФИО и дата рождения практически однозначно идентифицирует конкретного гражданина, и позволяют отнести их к конкретному субъекту, что является определением персональных данных. А наличие еще и медицинских данных в виде диагноза и особенностей заболевания абсолютно однозначно определяет конкретного субъекта, поэтому это система специальная класса К1, если строго следовать требованиям закона и подзаконных актов.

А как же тот факт, что по ФИО и дате рождения возможны совпадения, это же не паспортные данные или ИНН?

Тема 1.4. «Защита критической информационной инфраструктуры»

Промежуточная аттестация по теме «**Защита критической информационной инфраструктуры**» осуществляется в виде зачета, который включает в себя ответы на вопросы.

Оценка «зачтено» выставляется, если слушателем даны правильные, развернутые ответы.

Оценка «не зачтено» выставляется, если слушатель не ответил на вопрос, или ответил неправильно.

Примерные вопросы для промежуточной аттестации:

1. Реализация и эксплуатация. Приказ ФСТЭК 75
2. Защита КИИ. Нормативная база
3. Три кольца процессов КИИ
4. Административная ответственность в области КИИ
5. Уголовная ответственность в области КИИ

Тема 1.5. Эффективность защиты информации

Промежуточная аттестация по теме «Эффективность защиты информации» осуществляется в виде зачета, который включает в себя ответы на вопросы.

Оценка «зачтено» выставляется, если слушателем даны правильные, развернутые ответы.

Оценка «не зачтено» выставляется, если слушатель не ответил на вопрос, или ответил неправильно.

Примерные вопросы для промежуточной аттестации:

1. Факторы, способствующие развитию систем и средств обеспечения безопасности информации?
2. В каком соотношении по количеству проявлений угроз находятся такие угрозы как кража информации, халатность сотрудников, вирусные атаки?
3. Какие угрозы внешние или внутренние преобладают в настоящее время в информационных системах предприятий РФ.

Тема 1.6. Законодательство информационной безопасности

Промежуточная аттестация по теме «**Законодательство информационной безопасности**» осуществляется в виде зачета, который включает в себя ответы на вопросы.

Оценка «зачтено» выставляется, если слушателем даны правильные, развернутые ответы.

Оценка «не зачтено» выставляется, если слушатель не ответил на вопрос, или ответил неправильно.

Примерные вопросы для промежуточной аттестации:

1. Структура законодательства в РФ
2. Основания для прекращения ТД
3. Виды дисциплинарных взысканий
4. Материальная ответственность по ТК РФ
5. Информация как объект правовых отношений
6. Принципы обработки перс.данных
7. Условия обработки перс. Данных
8. Конфиденциальность перс. данных

Тема 1.7. Комплексное обеспечение информационной безопасности в интернет

Промежуточная аттестация по теме «Комплексное обеспечение информационной безопасности в интернет» осуществляется в виде зачета, который включает в себя написание эссе.

Оценка «зачтено» выставляется, если 50% объема эссе состоит из усвоенных знаний методического материалы и 50% отведено собственным комментариям, примерам и выводам автора. Объем эссе составляет не менее 1,5страниц.

Оценка «не зачтено» выставляется, если не соблюден объем эссе, нет собственных примеров, комментариев и выводов. Эссе представляет собой краткий обзор методических материалов, без выражения собственного мнения автора.

Примерные темы для написания эссе:

1. Информационные технологии и преступность. Понятие коберпреступности, киберпреступления и компьютерного преступления.
2. Виды киберпреступление. Кибертерроризм и информационные войны.
3. История международного сотрудничества в борьбе с кибепреступностью
4. Анализ проблем действующего законодательства о преступлениях в сфере компьютерной информации и возможных путей их решения

Итоговая аттестация

Итоговая аттестация проводится в форме итогового экзамена и не требует создание итоговой аттестационной комиссии, проводится одним из преподавателей реализующих данную программу.

Итоговая аттестация осуществляется в виде экзамена, который включает в себя выполнение итогового задания. Итоговая работа пишется на примере конкретной организации, где работает слушатель, и имеет практическую направленность.

Критерии оценки слушателя на итоговой аттестации:

Оценка «отлично» выставляется, если ответы соответствуют теме задания, заданному объему, полноте и обоснованности решения, полученные результаты соответствуют поставленной цели.

Оценки «хорошо» выставляется, если ответы соответствуют теме задания, есть недочеты по заданному объему, полноте и обоснованности решения, результаты соответствуют поставленной цели.

Оценки «удовлетворительно» выставляется, если ответы соответствуют теме задания, соблюдены требования к объему, нет обоснованности решения, полученные результаты не в полной мере соответствуют поставленной цели.

Оценка «неудовлетворительно» выставляется, если ответы не соответствуют теме задания, заданному объему, решение не обоснованно, полученные результаты не соответствуют поставленной цели.

Для получения оценки за итоговую аттестацию каждый слушателей подготавливает презентацию и презентует ее преподавателю.

В рамках подготовки презентации необходимо разработать Политику ИБ верхнего уровня и одну их подчиненных политик 2-го уровня.

5. ИНДИКАТОРЫ СФОРМИРОВАННЫХ КОМПЕТЕНЦИЙ ВЫПУСКНИКА ПРОГРАММЫ

В результате освоения программы у слушателя сформированы компетенции:

Таблица 5

Компетенция (код, содержание)	Индикаторы
Способен самостоятельно принимать обоснованные организационно-управленческие решения, оценивать их операционную, социальную значимость, обеспечивать их реализацию в условиях сложной (в том числе кросс-культурной) и динамичной среды (ОПК-3)	1. Владеет методами принятия оптимальных управленческих решений в условиях динамичной бизнес-среды. 2. Принимает обоснованные организационно-управленческие решения. 3. Оценивает операционную и организационную эффективность и социальную значимость организационно-управленческих решений.
Способность обоснования необходимости защиты информации в автоматизированной системе (ПСК-1)	1. Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах 2. Знает способы защиты информации от несанкционированного доступа и утечки по техническим каналам 3. Знает принципы построения систем защиты информации
Способность определения угроз безопасности информации, обрабатываемой автоматизированной системой (ПСК-2)	1. Знает Основные информационные технологии, используемые в автоматизированных системах 2. Знает Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях 3. Умеет Систематизировать результаты проведенных исследований

	4. Умеет Анализировать возможные уязвимости информационных систем 5. Владеет Программно-аппаратные средства обеспечения защиты информации автоматизированных систем
Способность разработки архитектуры системы защиты информации автоматизированной системы (ПСК-3)	1. Знает Основные информационные технологии, используемые в автоматизированных системах 2. Знает Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации 3. Умеет Определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах 4. Умеет Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем 5. Владеет методами Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы 6. Владеет Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем
Способность моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации (ПСК-4)	1. Знает Методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем 2. Знает Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах 3. Знает Национальные, межгосударственные и международные стандарты в области защиты информации 4. Умеет выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации 5. Умеет применять математические модели при проектировании систем защиты информации автоматизированных систем 6. Владеет разработкой аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем 7. Владеет методами исследования аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем