

Блоки экзаменационных вопросов

Блок 1 - теоретический - определяет уровень и системность теоретических знаний

Системы информационной безопасности

1. Актуальность и целесообразность аудита информационной безопасности, определения, терминология
2. Детализация направлений аудита информационной безопасности
3. Задачи комплексного, внешнего и внутреннего инструментального (активного) аудита информационной безопасности
4. Сбор информации при аудите информационной безопасности
5. Классы мер безопасности, направленные на людей
6. Неконтролируемый выход конфиденциальной информации за пределы контролируемой зоны, следствия выхода и виды угроз
7. Средства защиты, определяемые деятельностью человека или регламентирующие деятельность
8. Конфиденциальность, целостность, доступность информационной безопасности, способы обеспечения
9. Причины возникновения угроз безопасности информации
10. Компьютерные преступления. Этапы криминалистического процесса
11. Лог-файлы. Доказательная сила логов
12. Каким образом реализуется «Вредоносные программы», кто является преступником и какие следы остаются при реализации данного преступления
13. Каким образом реализуется «Мошенничество в онлайн играх», «Фишинг», кто является преступником и какие следы остаются при реализации данного преступления
14. Этичный хакинг
15. Инструменты этичного хакинга
16. Исследование восстановленных данных с помощью Kali Linux

Литература:

1. Лихоносов А., Денисов Д. Основы аудита информационной безопасности: учеб. пособие. – М.: МФПА, 2010. - 304 с.
2. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие / В.И. Аверченков. — 3-е изд. — М.: ФЛИНТА, 2016. — 269 с.
3. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - М.: Инфра-М. -2018. – 416 с.
5. Бузов Г.А. Защита информации ограниченного доступа от утечки

по техническим каналам. –М.: Горячая линия-Телеком, - 2015. - 585 с.

6. Мельников В. П. Защита информации: учеб. - М.: Академия, - 2014. - 304 с.

7. Нестеров С. А. Информационная безопасность: учеб. и практикум для акад. Бакалавриата. - М.: Юрайт, 2019. - 321 с

8. Федотов Н.Н. Форензика – компьютерная криминалистика –М.: Юридический Мир, 2007. – 432 с.

9. Kali Linux. Тестирование на проникновение и безопасность» Издательский дом Питер.

10. Common Vulnerability Scoring System SIG. URL: <https://www.first.org/cvss>

Блок 2 - практический - выявляет степень сформированности функциональных компетенций (умение применять методики, технологии и техники в предметной области)

Основные темы:

1. Методики тестирования информационных систем на защищенность от атак

2. Автоматизация расчета рисков при аудите информационной безопасности

3. Квалификационные требования к аудиторам информационной безопасности

4. Реализация политики информационной безопасности, организационные мероприятия защиты информации

5. Реализация политики информационной безопасности, мероприятия технического характера, обеспечивающие защиту объектов, людей и информации

6. Основные методики анализа рисков информационной безопасности, методы их оценки

7. Системы идентификации, применяющие биометрические характеристики

8. Средства защиты информации, основанные на преобразовании данных и обеспечивающие конфиденциальность и целостность информации

9. Приемлемые вопросы при проведении компьютерной технической экспертизы

10. Объекты исследования компьютерной криминалистической характеристики

11. Средства и инструменты компьютерной технической экспертизы

12. Заверение контента. Доказательство наличия контента. Выявление источника. Доказательство использования. Размещение в файловых сетях

13. Стандарты SysTrust и WebTrust.

Литература:

1. Лихоносов А., Денисов Д. Основы аудита информационной безопасности: учеб. пособие. – М.: МФПА, 2010. - 304 с.
2. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие / В.И. Аверченков. — 3-е изд. — М.: ФЛИНТА, 2016. — 269 с.
3. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - М.: Инфра-М. -2018. – 416 с.
5. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. –М.: Горячая линия-Телеком, - 2015. - 585 с.
6. Мельников В. П. Защита информации: учеб. - М.: Академия, - 2014. - 304 с.
7. Нестеров С. А. Информационная безопасность: учеб. и практикум для акад. Бакалавриата. - М.: Юрайт, 2019. - 321 с
8. Федотов Н.Н. Форензика – компьютерная криминалистика –М.: Юридический Мир, 2007. – 432 с.
9. Kali Linux. Тестирование на проникновение и безопасность» Издательский дом Питер.
10. Common Vulnerability Scoring System SIG. URL: <https://www.first.org/cvss>
11. ФСТЭК России. URL:<http://www.bdu.fstec.ru/>
12. <https://www.bsi.bund.de/>
13. <http://lib.itsec.ru/forum.php?sub=12011&from=-1>
14. Бубнов А., Пржегорлинский В., Савинкин О. Основы информационной безопасности. Учебник. –М.: Академия, – 2018. – 256 с.
15. Вострецова В.Е. Основы информационной безопасности: учебное пособие. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.
16. Bill Nelson, Amelia Phillips, Christopher Steuart Guide to Computer Forensics and Investigations: Processing Digital Evidence, Fifth Edition. Cengage Learning. 2016 WCN: 02-200-203

Блок 3 - выявляет системное понимание изучаемой предметной области, специализированные знания в области методологии исследования (системные компетенции)

Основные темы:

1. Требования к аудиторским компаниям в сфере информационных технологий.

2. Цель и назначение политики безопасности, содержание.
3. Количественные и качественные шкалы для определения величины риска информационной безопасности.
4. Определение защищенности и уровня информационной безопасности.
5. Обеспечение информационной безопасности, основные направления.
6. Аудит информационной безопасности, основные направления.
7. Критическая информационная инфраструктура, обеспечение защиты.
8. Технологии искусственного интеллекта и средства обеспечения комплексной безопасности.

Литература:

1. Аверченков, В.И. Аудит информационной безопасности: учеб. пособие / В.И. Аверченков. — 3-е изд. — М.: ФЛИНТА, 2016. — 269 с.
2. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - М.: Инфра-М. -2018. – 416 с.
4. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. –М.: Горячая линия-Телеком, - 2015. - 585 с.
5. Мельников В. П. Защита информации: учеб. - М.: Академия, - 2014. - 304 с.
6. Common Vulnerability Scoring System SIG. URL: <https://www.first.org/cvss>
7. ФСТЭК России. URL:<http://www.bdu.fstec.ru/>
8. <http://lib.itsec.ru/forum.php?sub=12011&from=-1>
9. Бубнов А., Пржегорлинский В., Савинкин О. Основы информационной безопасности. Учебник. –М.: Академия, – 2018. – 256 с.
10. Вострецова В.Е. Основы информационной безопасности: учебное пособие. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с.
11. Bill Nelson, Amelia Phillips, Christopher Steuart Guide to Computer Forensics and Investigations: Processing Digital Evidence, Fifth Edition. Cengage Learning. 2016 WCN: 02-200-203

Тематика Эссе

Проблемно-тематическое эссе по ГОП D 095

№	Эссе тақырыбы (қазақ тілінде)	Эссе тақырыбы (орыс тілінде)	Эссе тақырыбы (ағылшын тілінде)
---	----------------------------------	---------------------------------	------------------------------------

1	Ақпараттық қауіпсіздіктегі этика және жауапкершілік	Этика и ответственность в информационной безопасности	Ethics and responsibility in information security
2	Ағымдағы қызметіңіздің ақпараттық қауіпсіздік бағытымен байланысы	Корреляция вашей текущей деятельности с направлением информационной безопасности	Correlation of your current activity with the direction of information security
3	Жоспарланған диссертация тақырыбы. Осы тақырыптың өзектілігін негіздеңіз	Планируемая тема диссертации. Обоснуйте актуальность данной темы	The planned topic of the dissertation. Justify the relevance of this topic
4	Неліктен докторантураға түсуге шешім қабылдадыңыз? Қандай басылымдарыңыз бар, олардың деңгейі мен тақырыбы?	Почему решили поступать в докторантуру? Какие имеете публикации, их уровень и тематика?	Why did you decide to enroll in doctoral studies? What publications do you have, their level and subject matter?
5	Неліктен ақпараттық қауіпсіздік бойынша докторантураны таңдадыңыз? Сізде қандай ақпараттық қауіпсіздік дағдылары бар?	Почему выбрали докторантуру по информационной безопасности? Какие навыки в области информационной безопасности имеете?	Why did you choose a doctoral program in information security? What information security skills do you have?
6	Ақпараттық қауіпсіздіктің жеке және корпоративтік қауіпсіздікке әсері	Влияние информационной безопасности на личную и корпоративную безопасность	The impact of information security on personal and corporate security
7	Ақпараттық қауіпсіздіктегі этика және жауапкершілік	Этика и ответственность в информационной безопасности	Ethics and responsibility in information security

