УТВЕРЖДЕНО
на заседании Ученого совета
НАО «КазНУ им. аль-Фараби».
Протокол №14 от 16.06. 2026 г.

Программа вступительного экзамена для поступающих в докторантуру на группу образовательных программ D095 – «Информационная безопасность»

1. Общие положения.

1. Программа составлена в соответствии с Приказом Министра образования и науки Республики Казахстан от 31 октября 2018 года № 600 «Об утверждении Типовых правил приема на обучение в организации образования, реализующие образовательные программы высшего и послевузовского образования» (далее – Типовые правила).

2. Вступительный экзамен в докторантуру состоит из собеседования, написания эссе и экзамена по профилю группы образовательных программ.

Блок	Баллы
1. Собеседование	30
2. Эссе	20
3. Экзамен по профилю группы образовательной программы	50
Всего/проходной	100/75

3. Продолжительность вступительного экзамена - 3 часа 10 минут, в течение которых поступающий пишет эссе, отвечает на электронный экзаменационный билет. Собеседование проводится на базе вуза до вступительного экзамена.

2. Порядок проведения вступительного экзамена.

1. Поступающие в докторантуру на группу образовательных программ D095 -

«Информационная безопасность» пишут проблемное / тематическое эссе. Объем эссе – не менее 250-300 слов.

2. Электронный экзаменационный билет состоит из 3 вопросов.

Темы для подготовки к экзамену по профилю группы образовательной программы.

Дисциплина «Организация систем информационной безопасности»

Тема: Современные концепции и технологии обеспечения информационной безопасности

Подтемы:

1. Современные подходы к обеспечению информационной безопасности. Концепция Zero Trust Architecture. Принципы минимальных привилегий и непрерывной проверки доверия. Архитектура корпоративной безопасности в условиях цифровой трансформации. Исследовательская проблема формализации доверия в Zero Trust Architecture. Параметры контекста (пользователь, устройство, поведение, местоположение, риск сессии, чувствительность ресурса).
2. Исследовательский подход к построению модели зрелости процессов информационной безопасности на основе ISO/IEC 27001, NIST Cybersecurity Framework 2.0 и риск-ориентированного управления.
3. Архитектура и принципы функционирования Security Operations Center. Системы класса SIEM, SOAR, XDR и их применение для обнаружения и реагирования на инциденты. Научные проблемы при автоматизации реагирования на инциденты с использованием SIEM, SOAR и XDR. Оценка качества корреляции событий, приоритизации инцидентов и автоматических решений.
4. Управление киберрисками. Методологии идентификации, анализа и оценки рисков. Количественные и качественные методы оценки рисков. Построение моделей угроз. Отличия прикладной оценка риска от научной модели киберриска. Модель, учитывающая активы, угрозы, уязвимости, вероятность, ущерб, неопределённость и остаточный риск. Метрики для оценки снижения риска lateral movement, компрометации учётных записей, избыточных привилегий и несанкционированного доступа.
5. Кибербразведка (Cyber Threat Intelligence). Источники данных о киберугрозах. Таксономия угроз. Модель Cyber Kill Chain. Матрица MITRE ATT&CK и её использование при анализе атак. Сравните MITRE ATT&CK и Cyber Kill Chain как модели описания поведения противника.
6. Методы обнаружения компьютерных атак. Сигнатурные, эвристические и интеллектуальные методы обнаружения угроз. Системы IDS, IPS, NDR и EDR. Методология оценки качества обнаружения атак с учётом false positive, false negative, class imbalance, latency и стоимости ошибки.
7. Методы машинного обучения в задачах информационной безопасности. Обнаружение аномалий в сетевом трафике. Классификация атак с использованием методов искусственного интеллекта. Исследовательская проблема, обобщающая способности моделей машинного обучения для обнаружения сетевых атак. dataset shift, concept drift, дисбаланс классов и устаревшие датасеты влияющие на достоверность результатов

8. Глубокое обучение в системах кибербезопасности. Научные проблемы возникающие при применении CNN, RNN, LSTM, GRU и Transformer-моделей для обнаружения вторжений и анализа вредоносного программного обеспечения.

9. Нормативно – правовая документация Республики Казахстан. Обзор закона Республики Казахстан «О доступе к информации». Ограничения прав граждан Республики Казахстан, допущенных или ранее допускавшихся к государственным секретам Республики Казахстан. Статьи Уголовного Кодекса Республики Казахстан в сфере защиты персональных данных. Компетенции Правительства Республики Казахстан в сфере защиты персональных данных.

10. Методы выявления аудио-визуальных дипфейков. Архитектуры генеративных моделей. Методы детектирования синтетического контента. Оценка достоверности мультимедийных данных. Выявление аудио-визуальных deepfake техническая и методологическая проблема доверия к цифровым данным. Протокол оценки устойчивости deepfake detector к новым генеративным моделям, сжатию, шумам и неизвестным датасетам.

11. Облачная безопасность. Модели IaaS, PaaS и SaaS. Концепция Shared Responsibility Model. Управление безопасностью облачной инфраструктуры. Модель распределения киберрисков между cloud provider и cloud tenant в IaaS, PaaS и SaaS. Ограничения Shared Responsibility Model в multi-cloud и hybrid-cloud средах.

12. Безопасность контейнеризированных и микросервисных приложений. Технологии Docker и Kubernetes. Защита облачно-нативных приложений. Анализ данных с открытых источников и активные векторы атаки при получении доступа к закрытым источникам. Научная оценка рисков программной цепочки поставки в контейнеризированных приложениях. Уязвимости образов, registry, CI/CD pipeline, зависимостей, SBOM, подписи артефактов и политики допуска.

13. Безопасность Интернета вещей (IoT) и промышленных систем (IIoT). Уязвимости распределённых устройств. Методы защиты киберфизических систем. Новые научные проблемы возникают построения архитектуры информационной безопасности в условиях цифровой трансформации, удалённой работы, SaaS-сервисов, облаков, мобильных устройств и IoT.

14. Атрибуция кибератак. Методы идентификации источников атак. Использование Threat Intelligence, OSINT и поведенческого анализа для атрибуции. Эпистемологические и методологические ограничения при атрибуции кибератак. Неполнота данных, false flag, заимствование TTP, публичные инструменты, OSINT и уровни уверенности.

15. Перспективные направления развития информационной безопасности. Автономные системы защиты. Киберустойчивость. Искусственный интеллект в системах принятия решений по реагированию на инциденты. Научная проблема применения искусственного интеллекта в автоматизированном реагировании на инциденты.

Дисциплина «Элементы средств защиты информации»

Тема: защита информации компьютерных систем

Подтемы:

1. Архитектура современных компьютерных систем. Модели вычислительных систем (локальные, распределённые, облачные). Потоки данных в КС. Основные принципы обеспечения информационной безопасности в архитектуре системы.
2. Модель угроз в компьютерных системах. Классификация угроз: внутренние и внешние, преднамеренные и случайные. Каналы утечки информации. Модель нарушителя и его возможности. Оценка рисков информационной безопасности.
3. Механизмы контроля доступа в современных операционных системах. Дискреционные и мандатные модели доступа. Ролевое управление доступом (RBAC). Атрибутные модели (ABAC).
4. Современные методы идентификации и аутентификации пользователей. Биометрические технологии, многофакторная аутентификация, аппаратные токены. Протоколы аутентификации в распределённых системах.
5. Системы журналирования и мониторинга безопасности. Логирование событий безопасности, анализ журналов доступа. SIEM-системы и корреляция событий. Обнаружение аномальной активности.
6. Целостность данных в компьютерных системах. Методы контроля целостности файлов и процессов. Контрольные суммы, хэширование, цифровые подписи. Защита от модификации данных в реальном времени.
7. Программно-аппаратные средства защиты информации. Архитектура доверенных платформенных модулей (TPM). Аппаратные модули безопасности (HSM). Интеграция криптографических функций в аппаратное обеспечение.
8. Защита аппаратных компонентов компьютерных систем. Классификация защищаемых ресурсов: процессор, память, периферийные устройства. Методы защиты от физического доступа и атак на оборудование.
9. Защита программного обеспечения от несанкционированного копирования. Лицензирование программного обеспечения. Аппаратные ключи защиты. Привязка программ к аппаратной платформе и цифровым идентификаторам.
10. Управление секретной информацией в компьютерных системах. Хранение паролей и криптографических ключей. Безопасные хранилища (Key Vault, Secure Enclave). Политики управления секретами.
11. Жизненный цикл криптографических ключей. Генерация, распределение, хранение, ротация и уничтожение ключей. Централизованные и децентрализованные модели управления ключами (KMS).
12. Протоколы симметричной аутентификации и распределения ключей. Kerberos как пример централизованной системы аутентификации. Механизмы доверенного центра распределения ключей.

13. Протоколы асимметричной аутентификации. Использование инфраструктуры открытых ключей (PKI). Валидация сертификатов, цепочки доверия, отзыв сертификатов (CRL, OCSP).

14. Организация хранения и защиты ключевой информации. Аппаратные и программные носители ключей. Смарт-карты, токены, TPM-модули. Методы защиты ключей от извлечения и копирования.

15. Обратное проектирование программного обеспечения и защита от анализа. Методы статического и динамического анализа программ. Обфускация кода, антиотладочные механизмы, защита от дизассемблирования и реверс-инжиниринга.

Дисциплина **«Методы и средства защиты компьютерной информации»**

Тема: криптоанализ

Подтемы:

1. Классические шифры и их вскрытие. Шифр сдвига и афинный шифр и их дешифрование и взлом методом перебора. Частотный метод вскрытия шифра замены. Недостатки классических шифров, частотный анализ таких шифров текстов на казахском и русском языках.

2. Кольцо целых чисел, алгоритм Евклида и следствия. Представление наибольшего общего делителя. Теория сравнений. Свойства сравнений по данному модулю. Обратимые элементы по данному модулю.

3. Функция Эйлера и ее свойства. Функция Эйлера на простых числах. Теорема о мультипликативности функции Эйлера. Формула нахождения значений функции Эйлера, возведение в степень с использованием функции Эйлера.

4. Теорема Ферма-Эйлера и основная теорема RSA-шифра.

5. RSA-шифр, процесс шифрования и чтения, обоснование. RSA-шифрование открытым ключем заданного текста. RSA-дешифрование закрытым ключем заданного текста.

6. RSA-электронная подпись, идея и обоснование.

7. Реализация процедуры RSA-электронной подписи, часть подписывания электронной подписью документа.

8. Реализация процедуры RSA-электронной подписи, часть шифрование подписи открытым ключом.

9. Распределение простых чисел в натуральном ряду и оценка RSA шифра.

10. Кольцо многочленов над полем < F2 ; +,* > алгоритм Евклида, представление наибольшего общего делителя двух многочленов. Неприводимые многочлены в этом кольце. Неприводимые многочлены степеней 2,3,4,5.

11. Конструкция поля < F n ; +,* > как поля построенного из остатков по модулю неприводимого многочлен. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению

для ненулевых элементов этого поля. Построить поле < F16 ; +, * > .

12. Теорема Лагранжа о делимости порядка группы на порядок подгруппы. Следствия о том, что порядок элемента делит порядок группы. Примеры подгрупп группы Zn. Теорема о первообразном элементе в поле < F2n ; +,* >. Первообразные элементы поля < F16 ; +,* >.

13. Конструкция поля, построенного из n-разрядных двоичных блоков. Задание сложения и умножения в этом поле. Обратные элементы по сложению и обратные элементы по умножению для ненулевых элементов этого поля, первообразные элементы этого поля. Построить поле 4-разрядных двоичных блоков, указать первообразные элементы этого поля.

14. Задача Дифи-Хеллмана. Создание общего секрета для удаленных пользователей, опираясь на «неразрешимость» задачи Дифи-Хеллмана. Решение проблемы обмена ключами для удаленных пользователей.

15. Шифр Эль-Гамаля, прецесс обмена ключами, шифрование и дешифрования. Реализация на примере.

3. Список использованных источников.

1. Stallings W. *Cryptography and Network Security: Principles and Practice*. — 8th ed. — Pearson, 2020. — 768 p.
2. Katz J., Lindell Y. *Introduction to Modern Cryptography*. — 2nd ed. — CRC Press, 2014. — 538 p.
3. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. — CRC Press, 1996. — 816 p.
4. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. — 2nd ed. — Wiley, 1996. — 784 p.
5. Ferguson N., Schneier B., Kohno T. *Cryptography Engineering*. — Wiley, 2010. — 384 p.
6. Paar C., Pelzl J. *Understanding Cryptography*. — Springer, 2010. — 372 p.
7. Koblitz N. *A Course in Number Theory and Cryptography*. — Springer, 1994. — 236 p.
8. Diffie W., Hellman M. New Directions in Cryptography // *IEEE Transactions on Information Theory*. — 1976. — Vol. 22(6). — P. 644–654.
9. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // *Communications of the ACM*. — 1978. — Vol. 21(2). — P. 120–126.
10. ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // *IEEE Transactions on Information Theory*. — 1985. — Vol. 31(4). — P. 469–472.
11. Shannon C. E. Communication Theory of Secrecy Systems // *Bell System Technical Journal*. — 1949. — Vol. 28. — P. 656–715.
12. Bishop M. *Computer Security: Art and Science*. — Addison-Wesley, 2003. — 1134 p.

13. Pfleeger C., Pfleeger S. L. *Security in Computing*. — 5th ed. — Pearson, 2015. — 624 p.

14. Anderson R. *Security Engineering*. — 3rd ed. — Wiley, 2020. — 1250 p.

15. Easttom C. *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. — McGraw-Hill, 2021. — 600 p.

16. ISO/IEC 27001:2022. *Information Security Management Systems — Requirements*. — International Organization for Standardization, 2022.

17. ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*. — ISO, 2022.

18. Фомичев В. М. *Дискретная математика и криптография*. — М.: Диалог-МИФИ, 2012. — 400 с.

19. Ященко В. В. *Введение в криптографию*. — М.: МЦНМО, 2000. — 272 с.

20. Ожигов Ю. И. *Основы защиты информации в компьютерных системах*. — М.: Горячая линия-Телеком, 2018. — 320 с.