

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РЕСПУБЛИКИ КАЗАХСТАН**

**УЧРЕЖДЕНИЕ «ESIL UNIVERSITY»**



**ESIL**  
UNIVERSITY



Утверждаю

Ректор Учреждения «Esil University»

А.А. Таубаев

2026 г.

**ПРОГРАММА**

**комплексных экзаменов итоговой аттестации обучающихся  
по образовательной программе 6В06103 – «Информационные технологии  
и защита данных» по дисциплинам «Безопасность компьютерных  
сетей», «Проектирование защищенного ПО», «Криптографические  
методы защиты информации»**

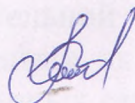
**Астана, 2026**

Программа комплексного экзамена (итоговой аттестации) разработана на основании Государственного общеобязательного стандарта высшего и послевузовского образования №2 от 20.07.2022 и модульных образовательных программ по ОП 6В06103 – «Информационные технологии и защита данных»

Программа комплексного экзамена (итоговой аттестации) обсуждена на заседании кафедры «Информационные системы и технологии»

Протокол № 6 от «16» 01 2026 г.

Заведующий кафедрой  
«Информационные системы и технологии»



А.Ұ. Мұхиядин

Программа одобрена на заседании Совета Факультета прикладных наук

Протокол № 6 от «19» 01 2026 г.

Председатель



А.А. Мухамеджанова

Программа одобрена на заседании Научно-методического Совета Учреждения «Esil University»

Протокол № 6 от «20» 01 2026 г.

Председатель



С.Б. Мақыш

Программа утверждена на заседании Ученого Совета Учреждения «Esil University»

Протокол № 8 от «23» 02 2026 г.

## ВВЕДЕНИЕ

О качестве подготовки студентов по образовательной программе 6B06103 – «Информационные технологии и защита данных» свидетельствуют результаты сдачи комплексного экзамена по специальным дисциплинам. Уровень усвоения студентом теоретического материала, предусмотренного учебной программой, должен определить комплексный экзамен, учитывающий общие требования к выпускнику, содержащиеся в государственном общеобязательном стандарте высшего и послевузовского образования по данной образовательной программе.

В комплексный экзамен по образовательной программе 6B06103 - «Информационные технологии и защита данных» включены вопросы по трем дисциплинам: «Безопасность компьютерных сетей», «Проектирование защищенного ПО», «Криптографические методы защиты информации». В программе указаны содержание тем, перечень вопросов и список рекомендуемой литературы в разрезе каждой дисциплины.

## **Программа по дисциплине «Безопасность компьютерных сетей»**

**Тема 1.** Основные понятия и определения дисциплины «Безопасность компьютерных сетей».

Понятия: информация, данные, актив, угроза, уязвимость, риск. Цели ИБ: конфиденциальность, целостность, доступность (CIA). Политика безопасности: назначение, структура, примеры требований. Меры защиты: организационные, технические, физические. Базовые принципы: минимальные привилегии, разделение обязанностей, защита в глубину

**Тема 2.** Введение в безопасность сетей Планирование безопасности сети и данных.

Задачи сетевой безопасности и область применения. Этапы планирования защиты: активы → угрозы → контроли → проверка. Проектирование политики доступа и правил пользования сетью. Модель Defense-in-Depth и слоистая защита. Подготовка к инцидентам: роли, процедуры, каналы уведомления

**Тема 3.** Сети для систем безопасности: оптимальные топологии

Топологии: звезда, кольцо, дерево, mesh, гибридные. Критерии выбора: надежность, отказоустойчивость, стоимость, масштабируемость. Зонирование и сегментация сети (DMZ, VLAN, зоны доверия). Резервирование каналов/устройств и высокая доступность (HA). Выделение отдельных сегментов для критичных сервисов и IoT/камер

**Тема 4.** Понятие периметра вычислительной сети. Модель OSI. Стандартные стеки коммуникационных протоколов.

Понятие периметра: границы сети, контроль входящего/исходящего трафика. Модель OSI: функции уровней и типовые угрозы по уровням. Стек TCP/IP и сопоставление с OSI. Коммуникационные протоколы и их роль в передаче данных. Где применяются средства защиты по уровням (фильтрация, шифрование, контроль доступа)

**Тема 5.** Модель TCP/IP. Сетевой протокол. Протокол TCP/ IP, DNS, ICMP

Уровни TCP/IP и их назначение. TCP и UDP: особенности, типовые угрозы и атаки. DNS: назначение, основные угрозы (подмена, отравление кэша). ICMP: функции диагностики и риски злоупотребления. Базовые меры защиты: ACL, ограничение ICMP, безопасная настройка DNS.

**Тема 6.** Обеспечение безопасности компьютерных сетей. Типы атак и уязвимость сетей.

Классификация атак: пассивные/активные, внешние/внутренние. Типовые атаки: MITM, spoofing, replay, session hijacking, DoS/DDoS. Понятия: уязвимость, эксплойт, поверхность атаки. Методы защиты: предотвращение, обнаружение, реагирование. Организационные меры: обучение, регламенты, контроль изменений.

**Тема 7.** Угрозы безопасности локальным и распределенным вычислительным сетям. Повышение уровня безопасности локальной вычислительной сети.

Отличия угроз LAN и WAN (перехват, подмена, инсайдерские риски).

Угрозы канального уровня в LAN (ARP/MAC/STP - на уровне введения). Сегментация LAN: VLAN, ACL, разделение сервисов и пользователей. Контроль доступа к сети: 802.1X/NAC (общее понимание). Hardening сетевых устройств, обновления, резервное копирование конфигураций

**Тема 8.** Механизмы безопасности на сетевых уровнях

Контроли на L2: Port Security, DHCP Snooping, Dynamic ARP Inspection, защита STP. Контроли на L3: anti-spoofing, ACL, защита маршрутизации. Контроли на L4: stateful inspection, управление портами/соединениями. Контроли на L7: WAF, прокси, фильтрация контента. Мониторинг и журналирование по уровням

**Тема 9.** Протоколы сетевой безопасности ssh, ssl, tls, smtp, l2f, ipsec, l2tp, pptp socks.

Назначение и область применения каждого протокола. SSH: защищенное администрирование, риски неправильной настройки. SSL/TLS: шифрование каналов, сертификаты, базовые принципы PKI. IPsec: режимы tunnel/transport, назначение IKE (общее). L2TP/PPTP/L2F/SOCKS: сценарии применения и ограничения безопасности

**Тема 10.** Защита беспроводной сети Безопасность в сетях WiFi. WEP, WPA, WPA2 шифрование.

Угрозы Wi-Fi: rogue AP, evil twin, sniffing, deauth. WEP: слабые места и причины отказа от использования. WPA/WPA2: PSK и Enterprise (общие отличия). Политика Wi-Fi: отдельные SSID (сотрудники/гости/IoT), сегментация VLAN. Мониторинг и обнаружение атак (WIDS/WIPS — общее), журналирование

**Тема 11.** Современные технологии защиты корпоративных сетей. Межсетевые экраны, системы обнаружения атак и виртуальные частные сети.

Межсетевые экраны: виды и место в архитектуре (perimeter/segmentation). IDS/IPS: назначение, различия, варианты размещения (SPAN/TAP/inline). VPN: сценарии (remote access/site-to-site), политика доступа. Интеграция: firewall + IDS/IPS + VPN + логирование (SIEM - общее). Практики: deny-by-default, управление изменениями, регулярный аудит правил

**Тема 12.** Внутренние злоумышленники в корпоративных сетях. Методы воздействия.

Типы внутренних нарушителей: случайные/неосторожные/умышленные. Методы: злоупотребление правами, утечки, саботаж, lateral movement. Контроли: least privilege, разделение ролей, PAM (общее понимание). Мониторинг: анализ поведения, журналы, контроль доступа к данным. Реагирование: расследование, фиксация доказательств, профилактика.

**Тема 13.** Концепция построения защищенных виртуальных частных сетей VPN.

Цели VPN: конфиденциальность, целостность, аутентификация. Архитектура: шлюзы, маршрутизация, точки доступа. Политики: MFA, роли и права, split tunneling и ограничения. Управление ключами/сертификатами (общее). Риски и ограничения: компрометация устройства, утечки, доверие клиенту

**Тема 14.** Сканеры уязвимостей Сетевые атаки Защита корпоративных сетей от внутренних злоумышленников.

Назначение сканеров уязвимостей и типовые результаты (отчеты). Виды сканирования: внутреннее/внешнее, аутентифицированное/без аутентификации. Приоритизация исправлений: по рискам и критичности активов. Remediation: исправление → повторная проверка → контроль изменений. Защита от инсайдеров: аудит, журналирование, сегментация, DLP (общее).

**Тема 15.** Противодействие пассивным методам воздействия Противодействие угрозе прослушивания сетевого трафика.

Пассивные воздействия: sniffing, анализ трафика, скрытый перехват. Риски: открытые сегменты, Wi-Fi, зеркалирование портов, TAP. Шифрование как основная мера: TLS, VPN, IPsec. Доп. меры: сегментация, защита коммутаторов, контроль портов. Обнаружение: аномалии, средства мониторинга, IDS/IPS (что могут/не могут)

### **Вопросы по дисциплине «Безопасность компьютерных сетей»**

1. Сетевые атаки, реализуемые на физическом уровне модели OSI
2. Атаки на коммутаторы: переполнение CAM-таблицы (CAM flooding), атаки на STP, MAC-spoofing, ARP-spoofing
3. Классификация (типология) сетевых средств защиты информации
4. Сети для систем безопасности: оптимальные топологии
5. Угрозы безопасности для локальных и распределённых вычислительных сетей. Повышение уровня безопасности LAN
6. Брандмауэр (Firewall): определение, виды
7. Системы обнаружения атак и VPN (взаимосвязь IDS/IPS и VPN)
8. Сетевые протоколы: TCP/IP, DNS, ICMP
9. Настройка VLAN в корпоративной сети
10. Многопользовательский режим работы: особенности и риски безопасности
11. Концепция построения защищённых виртуальных частных сетей (VPN)
12. Поиск различий между информацией, заявленной в исходных данных объекта информатизации, и фактически полученной информацией
13. Сетевые службы Windows Server, маршрутизация в ОС Windows
14. Защита сетевой инфраструктуры от несанкционированного доступа
15. Брандмауэр Microsoft Windows и особенности функционирования сетевых экранов в Интернете
16. Сканеры уязвимостей, сетевые атаки, защита корпоративной сети от внутренних нарушителей
17. Построение отказоустойчивой LAN на основе STP. Защита от атак на канальном уровне
18. Внутренние нарушители в корпоративных сетях: методы воздействия
19. Противодействие пассивным воздействиям: риск прослушивания сетевого трафика (sniffing)

20. Сравнение VPN-протоколов: SSH, IPsec, L2TP, PPTP
21. Критерии выбора VPN-протокола
22. Развёртывание домена и Group Policy (групповые политики)
23. Настройка протокола IP в корпоративной сети
24. Протокол сетевой безопасности IPsec и использование VPN
25. Криптографическая защита каналов передачи данных от несанкционированного доступа
26. Особенности выявления уязвимостей веб-приложений
27. Ограничение доступа и управление сетевыми ресурсами в сети Microsoft Windows
28. Проблемы безопасности современных корпоративных сетей
29. Аппаратное и программное обеспечение сети
30. Межсетевой экран нового поколения NGFW (Next-Generation Firewall)
31. Системное программное обеспечение сети
32. Угрозы протоколов TCP/IP (TCP/UDP)
33. Угрозы DNS: cache poisoning, spoofing, DNS-туннелирование - обнаружение и защита (DNSSEC/DoT/DoH)
34. ICMP: корректно ли полностью блокировать? Баланс риск/польза, какие типы следует разрешать?
35. IP-spoofing: как проявляется в сети и как строится anti-spoofing защита (uRPF, ACL)
36. Control Plane Protection: способы защиты плоскости управления маршрутизатора
37. Виды DDoS-атак (volumetric, protocol, application) и меры защиты для каждой
38. Межсетевой экран: функции, место в сети (периметр/сегментация) и принципы построения политики
39. Application firewall и WAF: отличия и какие угрозы веб-приложений они закрывают
40. NGFW: DPI, App-ID, IPS, URL-фильтрация, SSL-инспекция — какой механизм на какие угрозы отвечает
41. Система SIEM: назначение и принципы работы
42. Совместное использование IDS/IPS + VPN: где проверять VPN-трафик (до/после расшифрования туннеля)
43. IPsec: AH vs ESP и transport mode vs tunnel mode — различия и пример применения
44. Критерии выбора VPN-протокола: безопасность, поддержка, NAT traversal, производительность, масштабируемость
45. Выбор криптографических алгоритмов: AES, ChaCha20, RSA/ECDSA, DH/ECDH
46. В рамках Закона РК «Об информатизации» проанализируйте ключевые обязанности владельца/оператора ИС с точки зрения сетевой безопасности (защита, доступность, реагирование на инциденты)
47. Реализация требований Закона «О персональных данных и их защите» в сети: сбор/обработка/хранение, разграничение доступа,

- журналирование, риски передачи третьим лицам (предложите практические политики и технические меры)
48. В контексте Закона «О государственных секретах» как изменится архитектура сети? (изоляция, сегментация, уровни доступа, каналы передачи, рабочие станции для секретной информации)
  49. При конфликте требований Закона «О доступе к информации» и ИБ (открытость vs безопасность) предложите алгоритм принятия решения
  50. Назовите критерии разделения нарушителей на внутренних и внешних. Сравните их цели, возможности и уровень риска
  51. Дайте определение риска (risk) как «возможного ущерба при успешной реализации угрозы»
  52. Отличия качественной и количественной оценки рисков: когда и почему применяется каждая
  53. Как выполняется категорирование рисков (критический/ высокий/ средний/ низкий) и какие тактики управления применяются для каждой категории
  54. Как применять системный подход при построении карты рисков: выявление факторов, многоуровневый анализ, интеграция методов
  55. 4 стратегии обработки риска (avoid/reduce/transfer/accept) - объясните на примерах и назовите факторы выбора
  56. Что регулирует Закон РК «Об информатизации» в части создания/эксплуатации/защиты ИС? Какие обязанности возникают у организации?
  57. Какие требования предъявляет Закон РК «О персональных данных и их защите» к оператору при сборе/хранении/обработке/защите данных?
  58. Поясните значение Закона РК «О связи» в аспекте безопасности и взаимодействия с госорганами (инфраструктура, безопасность, защита, правоохранные аспекты)
  59. Этапы аудита ИБ (планирование → сбор информации → анализ → отчёт): какие методы/инструменты применяются на каждом этапе
  60. Внедрение NAC (Network Access Control): разработайте политику допуска BYOD/IoT/гостевых устройств (802.1X, posture check, quarantine VLAN, guest portal)
  61. Безопасность канала управления сетью: предложите схему (SSH, HTTPS, SNMPv3, AAA, management VLAN, out-of-band management)
  62. Безопасность SNMP и сетевого мониторинга: риски SNMPv2c, преимущества SNMPv3, опасные конфигурации и меры hardening
  63. Логирование и корреляция: архитектура сбора логов firewall/IDS/AD/DNS/VPN/Proxy (хранение, синхронизация времени/NTP, нормализация, пример корреляции)
  64. Сегментация сети vs микросегментация: сравните VLAN/ACL и policy-based microsegmentation; обоснуйте выбор для разных инфраструктур
  65. Проектирование DMZ: схема для внешних сервисов (веб-сервер/почта/DNS)
  66. Backup/DR (RPO/RTO): план восстановления корпоративной сети

- (критичность сервисов, резервные каналы, failover, тестирование)
67. DLP и предотвращение утечек (exfiltration): сравните меры контроля для e-mail/web/USB/VPN (DLP, CASB, proxy, firewall, UEBA)
  68. Безопасная настройка SSL/TLS: отключение слабых протоколов/шифров, управление сертификатами, влияние HSTS/OCSP stapling
  69. Защищённая почта и защита от фишинга: роль SPF/DKIM/DMARC, почтовый шлюз, sandbox, обучение пользователей - предложите интегрированную модель
  70. Сбор доказательств при инциденте: целостность журналов, chain of custody, синхронизация времени, порядок изоляции
  71. Сетевая безопасность приложений: reverse proxy/WAF, rate limiting, API gateway, mTLS - преимущества и ограничения (на сценарии web/API)
  72. Определите понятия: идентификация, аутентификация, авторизация, аудит. Цели каждого этапа и их связь
  73. Управление доступом к информации: сравнение моделей DAC, MAC, RBAC, ABAC и обоснование выбора модели для организации
  74. Почему идентификация по логину/паролю уязвима (фишинг, brute-force, социнженерия)? Предложите парольную политику и доп. меры защиты
  75. Разница между MFA, 2FA и однофакторной аутентификацией. Для каких систем что обязательно и почему
  76. Сравните биометрическую аутентификацию и токен/смарт-карту: безопасность, удобство, требования к инфраструктуре, риски приватности
  77. Механизмы авторизации: матрица доступа, ACL, capability-списки - сравните по масштабируемости и сложности отзыва прав
  78. Управление доступом в облаке: IAM, федерация, непрерывная верификация/Zero Trust. Почему периметрный подход недостаточен?
  79. Аудит и мониторинг доступа: какие поля обязаны быть в логах и почему важны целостность и централизованное хранение журналов
  80. PAM (Privileged Access Management): как реализуются least privilege, JIT-повышение прав, мониторинг/запись привилегированных сессий
  81. Модель OSI и стандартные стеки сетевых протоколов
  82. Современные технологии защиты корпоративных сетей
  83. Сегментация сети vs микросегментация: сравнение VLAN/ACL и policy-based microsegmentation, обоснование выбора
  84. Проектирование DMZ: схема, inbound/outbound правила и политика журналирования
  85. Сетевая защита от ransomware: остановка lateral movement (SMB/WinRM/RDP), сегментация, least privilege, backup (immutable/offline)
  86. Backup/DR (RPO/RTO): план восстановления корпоративной сети (критичность сервисов, резерв, failover, тестирование)
  87. Корпоративный дизайн Wi-Fi: несколько SSID (corp/guest/iot), разделение по VLAN, WPA2-Enterprise/WPA3, WIDS/WIPS, сценарий инцидента

88. Жизненный цикл управления уязвимостями: сканирование → привязка к рискам → устранение → повторная проверка. Достаточен ли CVSS?
89. Внедрение результатов pentest: включение уязвимостей в карту рисков, приоритизация и дорожная карта исправлений
90. Сбор доказательств при инциденте: целостность логов, chain of custody, синхронизация времени, порядок изоляции

### **Список рекомендуемой литературы**

#### **Основная литература**

1. Чернега, В. С. Методы и средства защиты периметра локальных компьютерных сетей: учебно-методическое пособие по выполнению лабораторных работ по дисциплине «Безопасность компьютерных сетей». – Севастополь: СевГУ, 2024. – 38 с. (электронный вариант: э-библиотека Esil University - <https://cloud.esil.edu.kz>).
2. Белоусова, Е. С. Основы построения локальных сетей. Лабораторный практикум: учебно-методическое пособие. – Минск: БГУИР, 2020. – 103 с.: ил. – ISBN 978-985-543-562-5. (электронный вариант: э-библиотека Esil University - <https://cloud.esil.edu.kz>).
3. Макаренко, С. И. Защита компьютерных сетей и телекоммуникаций: учебное пособие. – СПб.: Наукоемкие технологии, 2024. – 311 с. – ISBN 978-5-907618-79-4. (электронный вариант: э-библиотека Esil University - <https://cloud.esil.edu.kz>).
4. Мартынов, А. П.; Мартынова, И. А.; Русаков, А. А. Информационная безопасность и защита информации: учебное пособие. – 2-е изд. – Москва: Ай Пи Ар Медиа, 2024. – 130 с. – ISBN 978-5-4497-2349-9. (электронный вариант: э-библиотека Esil University - <https://cloud.esil.edu.kz>).
5. Платунова, С. М.; Елисеев, И. В.; Авксентьева, Е. Ю. Реализация комплексной безопасности в корпоративных сетях: шлюз безопасности как универсальное средство для обеспечения защиты данных и предотвращения вторжений. — СПб.: Университет ИТМО, 2020. – 64 с. (электронный вариант: э-библиотека Esil University — <https://cloud.esil.edu.kz>).

#### **Дополнительная литература**

1. Joseph Migga Kizza. Computer Communications and Networks. Springer London Heidelberg New York Dordrecht 2015 – 545 p. ISBN 978-1-4471-6653-5 ISBN 978-1-4471-6654-2 (eBook), DOI 10.1007/978-1-4471-6654-2
2. Н.А. Руденков [и др.]. Технологии защиты информации в компьютерных сетях: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. - 368 с. - ISBN 978-5-4497-0931-8. - Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - URL: <http://www.iprbookshop.ru/102069.html>

3. Фороузан Б.А. Криптография и безопасность сетей: учебное пособие / Фороузан Б.А. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. - 776 с. - ISBN 978-5-4497-0946-2.

4. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) Издательство «Горячая линия-Телеком» 2018

5. Олифер Виктор, Олифер Наталья О-54 Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. - СПб.: Питер, 2021. - 1008 с.: ил. - (Серия «Учебник для вузов»). ISBN 978-5-4461-1426-9

### **Программа по дисциплине «Проектирование защищенного ПО»**

**Тема 1.** Общие положения проектирования безопасных информационных систем

Понятие и назначение безопасных информационных систем. Принципы и этапы проектирования защищенного программного обеспечения. Роль безопасности на этапах жизненного цикла информационной системы. Основы методологии проектирования информационных систем.

**Тема 2.** Основы методологии проектирования информационных систем

Понятие методологии проектирования информационных систем. Структурный и объектно-ориентированный подходы. Модели жизненного цикла информационных систем: каскадная, итерационная, спиральная, гибкие методологии. Учет требований информационной безопасности в жизненном цикле.

**Тема 3.** Основы проектирования

Понятие проектирования информационных систем. Этапы и результаты проектирования. Функциональное моделирование. Назначение и особенности функциональной модели IDEF0 информационной системы.

**Тема 4.** Классификация информационной системы

Классификация информационных систем по назначению, масштабу, режиму обработки данных и уровню защищенности. Понятие актуальных угроз безопасности информации. Методика определения угроз. Разработка модели угроз информационной системы.

**Тема 5.** Функциональная модель IDEF0 информационной системы (AS-IS)

Назначение модели AS-IS. Построение функциональной модели текущего состояния информационной системы. Анализ процессов обработки информации и выявление уязвимых мест с точки зрения безопасности.

**Тема 6.** Требования к мерам и средствам защиты информации, применяемым в информационной системе

Требования к организационным, программным и техническим мерам

защиты информации. Требования к средствам защиты информации. Соответствие мер защиты выявленным угрозам и нормативным требованиям.

**Тема 7.** Функциональная модель IDEF0 информационной системы (ТО-ВЕ)

Назначение модели ТО-ВЕ. Проектирование целевого состояния информационной системы. Отражение мер защиты информации в функциональной модели. Сравнительный анализ моделей AS-IS и TO-BE.

**Тема 8.** Функциональная модель IDEF0 безопасной информационной системы (ТО-ВЕ)

Построение функциональной модели безопасной информационной системы. Интеграция механизмов защиты информации в процессы обработки данных. Обоснование выбора средств и мер защиты.

**Тема 9.** Диаграммы поведения Use Case безопасной информационной системы

Назначение диаграмм Use Case. Основные элементы диаграмм. Описание функций пользователей и администраторов. Использование диаграмм Use Case для анализа угроз и требований безопасности.

**Тема 10.** Установка и настройка средств защиты информации в информационной системе

Процессы внедрения средств защиты информации. Установка и настройка программных и аппаратных средств защиты. Разработка эксплуатационной документации. Документы, определяющие мероприятия по обеспечению защиты информации в ходе эксплуатации.

**Тема 11.** Диаграммы поведения Statechart безопасной информационной системы

Назначение диаграмм Statechart. Описание состояний и переходов в безопасной информационной системе. Использование диаграмм для моделирования поведения системы при реализации механизмов защиты.

**Тема 12.** Диаграммы поведения Activity безопасной информационной системы

Назначение диаграмм Activity. Моделирование процессов обработки информации и процессов обеспечения безопасности. Сравнение диаграмм Activity и Statechart.

**Тема 13.** Программа и методика аттестационных испытаний

Назначение аттестационных испытаний информационных систем. Структура программы и методики аттестации. Порядок проведения испытаний и оформления результатов.

**Тема 14.** Обеспечение безопасности среды эксплуатации информационной системы

Понятие среды эксплуатации информационной системы. Меры обеспечения безопасности среды эксплуатации. Администрирование системы защиты информации. Обязанности администратора безопасности.

**Тема 15.** Структурные диаграммы

Диаграммы классов и их назначение. Диаграммы развёртывания. Использование структурных диаграмм при проектировании защищенного

программного обеспечения. Архивирование информации конфиденциального характера. Уничтожение данных и остаточной информации с машинных носителей.

### **Вопросы по дисциплине «Проектирование защищенного ПО»**

1. Понятие безопасной информационной системы и её назначение.
2. Цели и задачи проектирования защищенного программного обеспечения.
3. Основные принципы проектирования безопасных информационных систем.
4. Роль информационной безопасности на этапах проектирования ИС.
5. Понятие методологии проектирования информационных систем.
6. Основные подходы к проектированию информационных систем.
7. Место безопасности в методологии проектирования ИС.
8. Понятие жизненного цикла информационной системы.
9. Основные модели жизненного цикла информационных систем.
10. Учет требований безопасности на различных этапах жизненного цикла ИС.
11. Понятие проектирования информационных систем.
12. Основные этапы проектирования информационной системы.
13. Назначение функционального моделирования при проектировании ИС.
14. Понятие функциональной модели информационной системы.
15. Нотация IDEF0 и её назначение.
16. Основные элементы функциональной модели IDEF0.
17. Правила построения диаграмм IDEF0.
18. Роль IDEF0 при проектировании защищенного ПО.
19. Классификация информационных систем по назначению.
20. Классификация информационных систем по масштабу и архитектуре.
21. Классификация информационных систем по уровню защищенности.
22. Понятие угроз безопасности информации.
23. Классификация угроз безопасности информации.
24. Понятие актуальных угроз безопасности информации.
25. Методика определения актуальных угроз безопасности информации.
26. Понятие модели угроз информационной системы.
27. Этапы разработки модели угроз.
28. Использование модели угроз при проектировании защищенного ПО.
29. Назначение модели AS-IS информационной системы.
30. Построение функциональной модели IDEF0 AS-IS.
31. Анализ уязвимостей на основе модели AS-IS.
32. Ограничения модели AS-IS при проектировании ИС.
33. Назначение целевой модели TO-BE информационной системы.
34. Отличие моделей AS-IS и TO-BE.

35. Отражение мер защиты информации в модели ТО-ВЕ.
36. Преимущества применения ТО-ВЕ при проектировании защищенного ПО.
37. Понятие безопасной информационной системы.
38. Особенности функциональной модели IDEF0 безопасной ИС.
39. Интеграция механизмов защиты информации в функциональные модели.
40. Обоснование выбора мер защиты в модели ТО-ВЕ безопасной ИС.
41. Требования к мерам защиты информации в информационной системе.
42. Требования к средствам защиты информации.
43. Соответствие мер защиты выявленным угрозам.
44. Учет нормативных требований при выборе средств защиты.
45. Понятие диаграмм поведения Use Case.
46. Назначение диаграмм Use Case в безопасной ИС.
47. Основные элементы диаграмм Use Case.
48. Использование Use Case для анализа требований безопасности.
49. Роль пользователей и администраторов в диаграммах Use Case.
50. Процессы установки средств защиты информации в ИС.
51. Настройка программных и технических средств защиты.
52. Этапы внедрения системы защиты информации.
53. Эксплуатационная документация по защите информации.
54. Документы оператора по обеспечению защиты информации.
55. Назначение диаграмм Statechart.
56. Отображение состояний безопасности информационной системы.
57. Использование Statechart для моделирования реакций системы.
58. Назначение диаграмм Activity.
59. Моделирование процессов обеспечения безопасности с помощью Activity.
60. Сравнение диаграмм Activity и Statechart.
61. Понятие программы и методики аттестационных испытаний.
62. Цели проведения аттестационных испытаний информационной системы.
63. Структура программы аттестационных испытаний.
64. Порядок проведения аттестационных испытаний.
65. Оформление результатов аттестационных испытаний.
66. Понятие среды эксплуатации информационной системы.
67. Основные угрозы безопасности среды эксплуатации ИС.
68. Меры обеспечения безопасности среды эксплуатации.
69. Администрирование системы защиты информации.
70. Функции администратора безопасности.
71. Понятие структурных диаграмм информационной системы.
72. Назначение диаграмм классов.

- 73.Использование диаграмм классов при проектировании защищенного ПО.
- 74.Назначение диаграмм развёртывания.
- 75.Отражение архитектуры ИС в диаграммах развёртывания.
- 76.Понятие архивирования информации конфиденциального характера.
- 77.Требования к архивированию конфиденциальной информации.
- 78.Процессы хранения архивной информации в ИС.
- 79.Понятие уничтожения информации.
- 80.Методы стирания данных с машинных носителей информации.
- 81.Уничтожение остаточной информации.
- 82.Требования к уничтожению машинных носителей информации.
- 83.Документирование процессов уничтожения информации.
- 84.Роль архивирования и уничтожения данных в системе защиты информации.
- 85.Комплексный подход к проектированию защищенного ПО.
- 86.Взаимосвязь функциональных, поведенческих и структурных моделей.
- 87.Ошибки при проектировании защищенных информационных систем.
- 88.Критерии оценки качества проектирования защищенного ПО.
- 89.Актуальные направления развития проектирования защищенных ИС.
- 90.Роль проектирования в обеспечении информационной безопасности организации

### **Список рекомендуемой литературы**

#### **Основная литература**

- 1 Duisebekova R.S. and etc. Database in IS: textbook / L.S. Korbossyn.- Almaty, 2016.-329 p.
- 2 Гвоздева Т.В. Проектирование информационных систем. Стандартизация: Учебное пособие / Т.В. Гвоздева Б.А. Баллод. - СПб.: Лань, 2019. - 252.
- 3 Дыбская В.В. Проектирование системы распределения в логистике: Монография / В.В. Дыбская. - М.: Инфра-М, 2019. - 277.
- 4 Конюх В.Л. Проектирование автоматизированных систем производства: Учебное пособие / В.Л. Конюх. - М.: Курс, 2018. - 64.
- 5 Трусев А.В. технология проектирования информационных систем: учебное пособие.-М.: Инфра-Инженерия, 2023.-244 с.

#### **Дополнительная литература**

- 1 Белов В.В. Проектирование информационных систем: Учебник / В.В. Белов. - М.: Академия, 2018. - 144.
- 2 Жук А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, 2А.И. Тимошкин. - М.: Риор, 2017. - 480 с.
- 3 Хетагуров Я.А. Проектирование автоматизированных систем обработки информации и управления (АСОИУ) / Я.А. Хетагуров. - М.: БИНОМ. Лаборатория знаний, 2015. - 240.

4 Хорольский В.Я. Проектирование и эксплуатация энергоустановок телекоммуникационных систем: Учебное пособие / В.Я. Хорольский, А.Б. Ершов. - М.: Форум, 2019. - 285.

5 Хорев П. Б. Программно-аппаратная защита информации. Учебное пособие. М.: Инфра-М. 2022. 327.

## **Программа по дисциплине «Криптографические методы защиты информации»**

**Тема 1.** Проблемы с защитой информации в компьютерной системе.

Основные проблемы защиты информации в современных компьютерных системах. Причины возникновения уязвимостей в компьютерных системах. Влияние человеческого фактора на уровень защиты информации. Последствия нарушений безопасности информации в компьютерных системах.

**Тема 2.** Правовая основа защиты информации.

Понятие и значение правовой основы защиты информации. Основные направления правового регулирования в сфере информационной безопасности. Ответственность за нарушение законодательства в области защиты информации. Роль нормативно-правовых актов в обеспечении информационной безопасности.

**Тема 3.** Основные проблемы безопасности автоматизированных систем обработки информации.

Криптографические принципы. Основные угрозы безопасности автоматизированных систем обработки информации. Особенности обеспечения безопасности автоматизированных систем обработки информации. Криптографические принципы информационного общества. Значение криптографии для защиты информации в автоматизированных системах обработки информации.

**Тема 4.** Основы и понятия криптографии.

Понятие криптографии и её основные задачи. Основные термины и понятия криптографии. Краткая история развития криптографии. Современное значение криптографии в системах защиты информации.

**Тема 5.** Криптография под ключ. Симметричные криптосистемы.

Понятие криптографии с секретным ключом. Принципы работы классических симметричных криптосистем. Преимущества и недостатки симметричного шифрования. Области применения симметричных криптосистем.

**Тема 6.** Симметричные алгоритмы.

Основные характеристики симметричных алгоритмов шифрования. Современные симметричные криптосистемы. Критерии криптостойкости симметричных алгоритмов. Режимы работы симметричных алгоритмов шифрования.

**Тема 7.** Система открытого распределения ключей.

Назначение системы открытого распределения ключей. Принципы функционирования систем распределения открытых ключей. Угрозы

безопасности при распределении криптографических ключей. Роль инфраструктуры открытых ключей в обеспечении безопасности.

#### **Тема 8. Система Диффи-Хеллмана.**

Назначение и принципы алгоритма Диффи-Хеллмана. Использование дискретных экспонент в системе Диффи-Хеллмана. Преимущества и ограничения алгоритма Диффи-Хеллмана. Угрозы и меры защиты при использовании Диффи-Хеллмана.

#### **Тема 9. Точность информации.**

Понятие точности информации и её значение. Факторы, влияющие на точность информации. Методы обеспечения и контроля точности информации. Последствия искажения информации в информационных системах.

#### **Тема 10. Аппаратное шифрование.**

Понятие и назначение аппаратного шифрования. Преимущества и недостатки аппаратных средств шифрования. Области применения аппаратного шифрования. Роль аппаратного шифрования в системе защиты информации.

#### **Тема 11. Программное шифрование.**

Понятие программного шифрования информации. Преимущества и недостатки программного шифрования. Сравнение аппаратного и программного шифрования. Использование программного шифрования в ИС.

#### **Тема 12. Операции с ключами.**

Жизненный цикл криптографического ключа. Основные операции с криптографическими ключами. Требования к хранению и защите ключей. Последствия компрометации криптографических ключей.

#### **Тема 13. Установление договора с помощью гамма-подхода.**

Понятие гамма-подхода в криптографии. Принципы установления защищённого договора. Преимущества и ограничения гамма-подхода. Применение гамма-подхода в системах защиты информации.

#### **Тема 14. Методы защиты от маргинального закрытия через Internet.**

Понятие маргинального закрытия и его угрозы. Методы защиты от атак через сеть Internet. Сетевые средства защиты информации. Комплексный подход к защите информации в Internet.

#### **Тема 15. Защита программ от исследований. Антивирусная защита.**

Методы защиты программного обеспечения от анализа. Понятие и виды антивирусной защиты. Принципы работы современных антивирусных средств. Роль антивирусной защиты в системе информационной безопасности.

### **Вопросы по дисциплине «Криптографические методы защиты информации»**

1. Понятие информационной безопасности и её основные цели.
2. Основные свойства информации: конфиденциальность, целостность и доступность.
3. Современные проблемы защиты информации в компьютерных системах.

4. Классификация угроз безопасности информации.
5. Внутренние и внешние угрозы информационной безопасности.
6. Уязвимости информационных систем и причины их возникновения.
7. Роль человеческого фактора в обеспечении защиты информации.
8. Последствия нарушений информационной безопасности.
9. Основные направления обеспечения информационной безопасности.
10. Комплексный подход к защите информации.
11. Правовая основа защиты информации в Республике Казахстан.
12. Основные нормативно-правовые акты в сфере информационной безопасности.
13. Понятие государственной, служебной и коммерческой тайны.
14. Ответственность за нарушение законодательства в области защиты информации.
15. Роль стандартов и регламентов в обеспечении информационной безопасности.
16. Организационные меры защиты информации.
17. Политика информационной безопасности организации.
18. Документационное обеспечение процессов защиты информации.
19. Контроль и аудит информационной безопасности.
20. Роль персонала в обеспечении защиты информации.
21. Понятие автоматизированной системы обработки информации.
22. Основные угрозы безопасности автоматизированных систем обработки информации.
23. Особенности защиты информации в автоматизированных системах обработки информации.
24. Классификация автоматизированных систем обработки информации по уровню защищённости.
25. Организационные и технические меры защиты автоматизированных систем обработки информации.
26. Модель угроз автоматизированной системы.
27. Угрозы нарушения конфиденциальности информации.
28. Угрозы нарушения целостности информации.
29. Угрозы нарушения доступности информации.
30. Роль криптографии в обеспечении безопасности информации.
31. Понятие криптографии и её основные задачи.
32. Основные термины и понятия криптографии.
33. История развития криптографии и основные этапы.
34. Криптографические принципы информационного общества.
35. Понятие криптографической стойкости.
36. Классификация криптографических методов защиты информации.
37. Шифрование как метод защиты информации.
38. Дешифрование и его назначение.
39. Место криптографии в системе информационной безопасности.
40. Ограничения и проблемы применения криптографии.
41. Понятие криптографии с секретным ключом.

42. Принцип работы симметричных криптосистем.
43. Классические симметричные алгоритмы шифрования.
44. Современные симметричные криптосистемы.
45. Преимущества симметричного шифрования.
46. Недостатки симметричных криптосистем.
47. Критерии оценки криптостойкости симметричных алгоритмов.
48. Режимы работы симметричных алгоритмов шифрования.
49. Области применения симметричных алгоритмов.
50. Роль симметричной криптографии в защите данных.
51. Понятие криптографического ключа.
52. Жизненный цикл криптографического ключа.
53. Основные операции с криптографическими ключами.
54. Генерация криптографических ключей.
55. Хранение и защита криптографических ключей.
56. Передача ключей по защищённым каналам связи.
57. Компрометация криптографических ключей и её последствия.
58. Обновление и отзыв криптографических ключей.
59. Политика управления криптографическими ключами.
60. Роль управления ключами в системе защиты информации.
61. Проблема распределения криптографических ключей.
62. Система открытого распределения ключей.
63. Принципы функционирования систем открытых ключей.
64. Инфраструктура открытых ключей (PKI).
65. Назначение и основные компоненты PKI.
66. Алгоритм Диффи–Хеллмана и его назначение.
67. Использование дискретных экспонент в алгоритме Диффи–Хеллмана.
68. Преимущества и ограничения алгоритма Диффи–Хеллмана.
69. Угрозы безопасности при распределении ключей.
70. Способы защиты каналов распределения ключей.
71. Понятие и назначение аппаратного шифрования.
72. Преимущества аппаратных средств шифрования.
73. Недостатки аппаратных средств шифрования.
74. Понятие программного шифрования информации.
75. Преимущества программного шифрования.
76. Недостатки программного шифрования.
77. Сравнительная характеристика аппаратного и программного шифрования.
78. Выбор средств шифрования для информационных систем.
79. Влияние шифрования на производительность системы.
80. Роль шифрования в комплексной системе защиты информации.
81. Понятие точности информации и её значение.
82. Факторы, влияющие на точность информации.
83. Методы обеспечения целостности информации.
84. Контроль целостности и точности данных.
85. Понятие защиты программного обеспечения от анализа.

86. Методы защиты программ от исследований и реверс-инжиниринга.
87. Понятие антивирусной защиты.
88. Виды антивирусных программ.
89. Принципы работы современных антивирусных средств.
90. Роль антивирусной защиты в системе информационной безопасности.

### **Список рекомендуемой литературы**

#### **Основная литература**

1. Peter H. Gregory Blocking Spam For Business For Dummies® (For Dummies (Computers)) / Peter H. Gregory. - Москва: ИЛ, 2016. - 636 с.
2. Бабаш А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2016. - 240 с.
3. Бабенко Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.
4. Бабенко Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 с.
5. Бузов Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 с.

#### **Дополнительная литература**

1. Зубов А.Н. Математика кодов аутентификации / А.Н. Зубов. - М.: Гелиос АРВ, 2014. - 319 с.
2. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2014. - 496 с.
3. Кузьмин Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2013. - 192 с.
4. Литвинская О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 с.
5. Осмоловский С. А. Стохастическая информатика. Инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия - Телеком, 2012. - 322 с.