**Итоговый тест курса**

**«Подготовка к собеседованию специалиста по информационной безопасности»**

|  |  |  |
| --- | --- | --- |
| № п\п | Формулировка вопроса | Варианты ответов |
| Основные стандарты, требования, положения законодательства и регуляторов. Руководящие документы | | |
| 1 | Какие документы относится к регуляторным требованиям в области ИБ? | 1. Приказ ФСТЭК России от 25 декабря 2017 г. N 239.  2. Доктрина информационной безопасности Российской Федерации.  3. Федеральный закон N 187-ФЗ от 26 июля 2017 года "О безопасности критической информационной инфраструктуры Российской Федерации".  4. Приказ ФСБ России от 10 июля 2014 г. N 378. |
| 2 | Какая серия стандартов регулирует деятельность по ИБ с учетом внедрения лучших практик и рекомендаций для создания , развития и поддержания системы менеджмента ИБ? | 1. ГОСТ Р 50739.  2. ГОСТ Р ИСО/МЭК 29100.  3. ГОСТ Р ИСО/МЭК 27000.  4. Р 50.1.053-2005. |
| 3 | По каким основным параметрам классифицируются виды угроз ИБ? | 1. Конфиденциальность-Целостность-Доступность.  2. Конфиденциальность-Подотчетность-Резидентность.  3. Уникальность-Востребуемость-Идентичность.  4. Возобновляемость-Конфиденциальность-доступность. |
| 4 | Что можно отнести к отраслевым стандартам в области ИБ? | 1. Международное законодательство.  2. Приказы МинЮста.  3. Постановления Верховного Суда.  4. Стандарты Банка России. |
| Основные стандарты, требования, положения международного законодательства. Best practice | | |
| 1 | В соответствии с какой методикой обычно проводят повышение осведомленности пользователей в вопросах ИБ? | 1. SANS.  2. OWASP.  3. CIS.  4. ITIL. |
| 2 | Что относится к международному законодательству в области ИБ? | 1. PCI DSS.  2. SOX.  3. GDPR.  4. LOPD. |
| 3 | Какими стандартами обеспечивается управление ИБ? | 1. NIST SP800-94 - Cisco SAFE - ISO27004 - NIST SP800-41.  2. BS 7799-3:2006 - Cisco SAFE - ISO27004 - NIST SP800-41.  3. NIST SP800-86 - ISO27000-2 – NSA – ISACA.  4. ISO/IEC 18028-4:2005 – OWASP – SOX - ISO27003. |
| 4 | Какое из основных направлений ИБ пропущено цепочке:  1. Обеспечение и управление ИБ.  2. Управление рисками.  3. Аудит IT и ИБ.  4. Управление IT.  5. Непрерывность бизнеса.  6. Повышение осведомленности.  7. Рекомендации для проектирования защиты.  8. Рекомендации по ИБ (личные). | Обработка инцидентов ИБ |
| Информационные системы обеспечения информационной безопасности и средства защиты | | |
| 1 | Перечислите методы борьбы с вирусами | 1. Сигнатурный.  2. Эвристический.  3. Брандмауэрный. |
| 2 | DLP-системы разделяются по способам обнаружения каналов утечек чувствительной информации при: | 1. Хранении чувствительной информации.  2. Использовании чувствительной информации.  3. При резервировании чувствительной информации.  4. Передаче чувствительной информации. |
| 3 | В чем основное отличие APT от WAF? | APT позволяет выстроить защиту от целевой атаки, направленной в т.ч. для обхода WAF и IPS. |
| 4 | Выберите не верный класс сканеров безопасности. | 1. Сканеры безопасности сетевых сервисов и протоколов.  2. Сканеры инфраструктуры.  3. Сканеры безопасности реестра операционных систем.  4. Сканеры безопасности приложений.  5. Сканеры безопасности исходного кода. |
| 5 | Что необходимо для разворачивания SIEM? | 1. Логи.  2. Сигналы тревоги.  3. Информация об инфраструктуре.  4. Информация о средствах защиты информации. |
| 6 | В чем отличие SAOR от SIEM? | SOAR – это специальный инструмент агрегирования информации об угрозах безопасности с последующим их анализом и на основании результатов работы SIEM. |
| 7 | Какой вид IDS указан не верно? | 1. NIPS.  2. APIDS.  3. NIDS.  4. HIDS. |
| 8 | Какой регулятор регламентирует сертификацию средств от НСД? | 1. ФСБ.  2. РКН.  3. ФСТЭК.  4. ФАПСИ. |
| 9 | Какие классы СКЗИ наверняка существуют? | 1. КС1-КС2-КВ2-КА1.  2. КС3-КВ1-КВ2-КА2.  3. КВ1-КВ2-КС4-КС1.  4. КВ-КС-КА-КЕ. |
| 10 | Что не реализует SOC-центр на этапе сканирования и оценки защищенности? | 1. Создание и актуализация карты сети.  2. Сканирование уязвимостей.  3. Оценка защищенности.  4. Оценка угроз. |
| 11 | Что не реализует antifraud-система при аналитике событий? | 1. Контроль аутентификации.  2. Предварительная обработка.  3. Оценка риска.  4. Принятие решений на основе правил. |
| 12 | Какие случаи являются предпосылками к аналитике кода? | 1. Переполнение буфера ПО.  2. Повышение привилегий.  3. Наличие ошибок форматных строк.  4. Наличие «полезной нагрузки». |
| IT-инновации в бизнесе. Модели, виды, системы. Уязвимости, подходы к защите и аналитика | | |
| 1 | Перечислите основные направления обеспечения конфиденциальности данных в BigData: | 1. Сохранение конфиденциальности при обработке и анализе данных.  2. Определение происхождения данных.  3. Система безопасности данных, усиленная криптографией.  4. Гранулированный контроль доступа. |
| 2 | Какие направления пентестинга можно автоматизировать с помощью NN? | 1. Социальная инженерия.  2. Инспекция вредоносного кода.  3. Дебагинг.  4. Фаззинг. |
| 3 | Что не относится к уязвимостям клиентской части приложения? | 1. Небезопасное межпроцессорное взаимодействие.  2. Недостатки конфигурации и резервные копии.  3. Использование клавиатурных расширений.  4. Сочетание XSS и trace-запросов. |
| 4 | Какого типа угроз не существует для среды виртуализации? | 1. Угрозы платформы виртуализации.  2. Угрозы, связанные с конфигурацией виртуальной среды.  3. Классические угроз IT-инфраструктуры, реализованной в виртуальной среде.  4. Уязвимости коммуникационной экосистемы. |
| DevSecOps. Роль эксперта в области защиты информации при кросс-функциональном взаимодействии | | |
| 1 | Какие процессы характерны для этапа Design в SDLC | 1. Core security training.  2. Dynamic analysis – Fuzz testing – Attack surface review  3. Establish design requirements – Analyze Attack surface – Threat Modeling  4. Use Approved Tools – Deprecate Unsafe Functions – Static Analysis |
| 2 | POC с точки зрения ИБ – это: | 1. Формирование экспертизы (базы знаний) стандартных сценариев ИБ к проекту.  2. Формулировка целей и задач ИБ.  3. Обеспечение тестирования безопасности.  4. Автоматизированное тестирование и сканирование безопасности. |
| 3 | Что не выявляется на этапе DAST? | 1. Утечки памяти.  2. Перерасход ресурсов.  3. Лицензионные ограничения.  4. Ошибки аутентификации. |