pt career hub

МАТРИЦА КОМПЕТЕНЦИЙ В ОБЛАСТИ КИБЕР-БЕЗОПАСНОСТИ

Матрица компетенций в области кибербезопасности

Безопасная разработка программного обеспечения

- **Управление рисками**
  - Уполномоченный по рискам информационной безопасности или его ответственный представитель. Если в компании есть комиссия по рискам, уполномоченным может быть ИТ-директор, технический директор или директор по продуктам
- **Разработка программного обеспечения**
  - Эксперт по оценке мер информационной безопасности инфраструктуры
  - Разработчик программного обеспечения
  - Эксперт по оценке безопасности программного обеспечения
- **Архитектура корпоративных информационных систем**
  - Архитектор корпоративных информационных систем
  - Архитектор систем безопасности
- **Разработка информационных систем**
  - Разработчик систем защиты информации
  - Разработчик корпоративных информационных систем
- **Планирование системных требований**
  - Аналитик системных требований
- **Технологические исследования и разработки**
  - Специалист по безопасной разработке
- **Тестирование и оценка ПО**
  - Специалист по тестированию и оценке ПО

Старшее должностное лицо или руководитель, имеющий полномочия официально взять на себя ответственность за эксплуатацию информационной системы при приемлемом уровне риска для деятельности организации (в том числе для миссии, функций, имиджа или репутации), активов организации, отдельных лиц, других организаций и государства

Проводит независимую комплексную оценку управленческих, организационных и технических мер безопасности и дополнительных средств контроля, используемых в ИТ-системах или унаследованных от ее предыдущей версии, для определения общей эффективности мер безопасности

Разрабатывает, создает, поддерживает и пишет новое (или модифицирует существующее) программное обеспечение, в том числе прикладные или специализированные служебные программы

Анализирует безопасность нового или уже существующего программного обеспечения, в том числе прикладных или специализированных служебных программ, и делает выводы, значимые для дальнейших действий

Разрабатывает и поддерживает бизнес-процессы, системные подходы и информационные процессы, способствующие успешному выполнению миссии организации

Разрабатывает правила и требования в сфере ИТ, которые описывают базовую и целевую архитектуру

Обеспечивает возможность того, чтобы требования к безопасности, определенные заинтересованными сторонами и необходимые для осуществления миссии и бизнес-процессов организации, были адекватно учтены во всех аспектах архитектуры корпоративных систем, включая эталонные модели, архитектуру сегментов и решений, а также итоговые системы, поддерживающие стратегические задачи и бизнес-процессы организации

Проектирует, разрабатывает, тестирует и оценивает аспекты безопасности информационных систем на протяжении всего жизненного цикла разработки систем

Проектирует, разрабатывает, тестирует и оценивает информационные системы на протяжении всего жизненного цикла разработки систем

Взаимодействует с заказчиками, чтобы оценивать функциональные требования и преобразовывать их в технические решения

Занимается системной и программной инженерией, исследует системы ПО для разработки новых возможностей с полной интеграцией аспектов кибербезопасности

Проводит комплексные технологические исследования для оценки потенциальных уязвимостей цифровых систем

Планирует, готовит и проводит испытания систем для оценки результатов на соответствие техническим заданиям и требованиям, а также анализирует результаты испытаний и излагает их в отчетах

Мониторинг событий ИБ и реагирование на инциденты ИБ

- **Мониторинг инцидентов информационной безопасности**
  - Аналитик центра мониторинга информационной безопасности
- **Поддержка инфраструктуры информационной безопасности**
  - Специалист по поддержке инфраструктуры информационной безопасности
- **Реагирование на инциденты информационной безопасности**
  - Специалист по реагированию на инциденты информационной безопасности
- **Оценка и управление уязвимостями**
  - Аналитик по оценке уязвимостей (пентестер)

Использует данные, собранные с помощью различных средств киберзащиты (например, оповещения систем обнаружения вторжений (IDS), данные межсетевых экранов, журналы сетевого трафика, для анализа событий с целью нейтрализации угроз

Тестирует, внедряет, развертывает, обслуживает и администрирует аппаратное и программное обеспечение инфраструктуры киберзащиты

Расследует и анализирует инциденты информационной безопасности в сетевой среде или изолированном сегменте, реагирует на них

Выполняет оценку систем и сетей в рамках сетевой среды или анализа и обнаруживает отклонения от допустимых конфигураций, политики изолированного сегмента или локальной политики

Измеряет эффективность многослойной архитектуры защиты от известных уязвимостей

Нормативно- правовое обеспечение и организационные меры информационной безопасности

- **Обеспечение ИБ**
  - Аналитик безопасности систем (методолог)
  - Менеджер по безопасности связи (специалист удостоверяющего центра)
  - Менеджер по безопасности информационных систем
- **Управление ИБ**
  - Руководитель направления информационной безопасности (CISO)
- **Нормативно- правовое обеспечение ИБ**
  - Юридический советник по вопросам информационной безопасности
  - Менеджер по вопросам защиты конфиденциальной информации
- **Управление проектами**
  - Управляющий портфелем инвестиций в ИТ
  - Аудитор проектов ИТ и ИБ
  - Менеджер проектов ИТ и ИБ
  - Менеджер по поддержке продуктов
  - Руководитель проектов
- **Стратегическое планирование и управление**
  - Специалист по разработке политики и стратегии в сфере информационной безопасности (заместитель CISO)
  - Менеджер по развитию персонала в сфере информационной безопасности (HR)
- **Обучение, образование и повышение квалификации**
  - Разработчик учебных программ по информационной безопасности
  - Преподаватель по информационной безопасности (преподаватель по киберграмотности)

Отвечает за анализ и разработку документации по интеграции, тестированию, реализации и поддерживанию мер безопасности систем

Лицо, управляющее ресурсами безопасности связи в организации или ответственное за хранение ключей системы управления криптографическими ключами (crypto key management system, CKMS)

Отвечает за киберзащищенность проекта, системы и организации (дочерней организации)

Принимает решения, формирует стратегическое видение и осуществляет общее управление ресурсами и деятельностью организации в сфере кибербезопасности и цифровых технологий

Предоставляет юридические консультации и рекомендации по актуальным темам, связанным с законодательством в сфере кибербезопасности

Разрабатывает и контролирует программу соблюдения требований к конфиденциальности персональных данных, курирует работу персонала, занятого в программе

Оказывает поддержку по вопросам соблюдения законодательства, корпоративного управления и политики в сфере конфиденциальности данных, в ранее при реагировании на инциденты

Управляет портфелем инвестиций в информационные технологии, которые соответствуют общим заданиям и приоритетам организации

Оценивает ИТ-программы или их отдельные компоненты на соответствие опубликованным стандартам информационной безопасности

Непосредственно руководит проектами в области информационных технологий и информационной безопасности

Управляет вспомогательными функциями, необходимыми для эксплуатации и поддержания готовности и работоспособности систем и компонентов

Осуществляет руководство, координацию, коммуникацию, интеграцию и несет ответственность за общий успех программы, обеспечивая согласованность с приоритетами организации

Разрабатывает и поддерживает в актуальном состоянии планы, стратегию и политику информационной безопасности, чтобы реализовать инициативы организации в области информационной безопасности и обеспечивать соблюдение нормативных требований

Разрабатывает планы, стратегии и рекомендации по кадровым ресурсам в сфере информационной безопасности, чтобы удовлетворять потребности в квалифицированном персонале с учетом изменений в политике, основополагающих принципах деятельности, материально- технических ресурсах, организационной структуре и требованиях к обучению и подготовке

Разрабатывает, планирует, координирует и оценивает курсы, методы и технологии обучения и подготовки в области информационной безопасности, опираясь на методические потребности

Разрабатывает и проводит тренинги или обучение персонала в сфере информационной безопасности

Эксплуатация и техническое обслуживание информационных систем

- **Обслуживание клиентов и техническая поддержка**
  - Специалист службы технической поддержки
- **Администрирование данных**
  - Технический специалист по анализу данных
  - Администратор баз данных
- **Управление базой знаний**
  - Специалист по развитию базы знаний
- **Эксплуатация сетей**
  - Специалист по эксплуатации сетей
- **Системное администрирование**
  - Системный администратор
- **Системный анализ**
  - Аналитик безопасности систем

Оказывает техническую поддержку пользователям, которым требуется помощь в использовании аппаратного и программного обеспечения на клиентском уровне, в соответствии с установленными процессами и утвержденными документами организации (например, генеральным планом управления инцидентами, если применимо)

Изучает данные из многочисленных разрозненных источников и предоставляет аналитические выводы о безопасности и конфиденциальности

Разрабатывает и внедряет специализированные алгоритмы, рабочие процессы и схемы для сложных наборов данных корпоративного масштаба, используемые для моделирования, интеллектуального анализа данных и исследований

Администрирует базы данных и (или) системы управления данными, которые обеспечивают безопасное хранение, запрос, защиту и использование данных

Отвечает за управление процессами и администрирование инструментов, которые позволяют организации идентифицировать, документировать и использовать интеллектуальный капитал и информационные материалы

Планирует, внедряет и эксплуатирует сетевые службы и системы, включая физические и виртуальные среды

Отвечает за настройку и обслуживание системы или определенных компонентов системы (например, за установку, настройку и обновление аппаратного и программного обеспечения, создание учетных записей пользователей и управление ими; надзор за резервным копированием и восстановлением или самостоятельное выполнение этих задач; внедрение организационных и технических мер безопасности; соблюдение политики и процедур безопасности организации)

Отвечает за анализ и разработку документации по интеграции, тестированию, реализации и поддерживанию мер безопасности систем

Аналитика ИБ

- **Анализ данных из разнородных источников**
  - **Аналитик данных в сфере информационно-аналитического обеспечения**
    - Анализирует данные и информацию из одного или нескольких источников, чтобы обеспечить понимание оперативной обстановки
    - Отвечает на запросы о предоставлении информации
    - Формирует задания по сбору и подготовке данных в поддержку планирования и проведения мероприятий
  - **Специалист по информационно-аналитическому обеспечению**
    - Разрабатывает планы оценки и показатели эффективности
    - Оценивает стратегическую и оперативную эффективность мероприятий по кибербезопасности
    - Определяет, работали ли системы так, как ожидалось, и предоставляет данные для определения операционной эффективности
- **Анализ эксплуатации уязвимостей информационных систем**
  - **Аналитик данных в области эксплуатации уязвимостей информационных систем**
    - Совместно с другими специалистами определяет пробелы в доступе и информации, которые можно заполнить посредством эксплуатации уязвимостей и сбора данных в киберпространстве
    - Использует все разрешенные ресурсы и аналитические методы для проникновения в целевые сети
- **Языковой анализ данных**
  - **Многопрофильный аналитик-лингвист**
    - Применяет знания в сфере языков, культуры и техники, а также знания об угрозах и целевых объектах, чтобы обрабатывать, анализировать и (или) распространять информацию, извлеченную из языковых, голосовых и графических материалов
    - Создает и поддерживает базы данных и рабочие пособия по конкретным языкам для реализации мероприятий по кибербезопасности и обмена взаимодействия знаниями
    - Предоставляет экспертные знания в рамках межведомственных проектов или проектов, в которых активно используются иностранные языки
- **Анализ целевых информационных систем**
  - **Аналитик данных об уязвимостях эксплуатируемой программного обеспечения (разведка)**
    - Анализирует целевые системы, создает и (или) ведет электронные папки целевых объектов, наполняя их данными, полученными в ходе изучения обстановки и (или) из внутренних или внешних источников оперативной информации
    - Координирует действия относительно целевых объектов с партнерами и разведывательными организациями, предоставляет кандидатуры целевых объектов для проверки и подтверждения
  - **Аналитик данных об уязвимостях эксплуатируемой сетевой инфраструктуры (разведка)**
    - Проводит углубленный анализ собранных данных и данных из открытых источников, чтобы обеспечивать стабильную работу с целевыми объектами, составить профили целевых объектов и их деятельности, а также разрабатывать методы получения дополнительной информации о целевых объектах
    - Определяет, как общаются, перемещаются, действуют и живут целевые объекты, основываясь на знании технологий, цифровых сетей и приложений, используемых целевыми объектами
- **Прогнозирование угроз информационной безопасности**
  - **Аналитик данных об угрозах ИБ**
    - Разрабатывает индикаторы киберугроз для поддержания осведомленности о динамично меняющейся обстановке
    - Собирает, обрабатывает, анализирует и распространяет оценки киберугроз и предупредительные сигналов

Сбор данных и эксплуатация уязвимостей информационных систем

- **Сбор данных из разнородных источников**
  - **Специалист по сбору данных из открытых источников (OSINT, threat hunting)**
    - Включает приоритетные информационные запросы в программу сбора данных
    - Разрабатывает концепции для выполнения намерений руководства
    - Определяет возможности имеющихся средств сбора данных, выявляет новые возможности сбора данных
  - **Специалист по сбору данных из закрытых источников**
    - Включает приоритетные информационные запросы в программу сбора данных
    - Разрабатывает концепции для выполнения намерений руководства
    - Определяет возможности имеющихся средств сбора данных, выявляет новые возможности сбора данных
  - **Специалист по сбору данных из социальных сетей**
    - Включает приоритетные информационные запросы в программу сбора данных
    - Разрабатывает концепции для выполнения намерений руководства
    - Определяет возможности имеющихся средств сбора данных, выявляет новые возможности сбора данных
  - **Руководитель подразделения по сбору данных из разнородных источников**
    - Определяет, где и с помощью каких уполномоченных служб можно собрать необходимые данные
    - Включает приоритетные информационные запросы в программу сбора данных
    - Разрабатывает концепции для выполнения намерений руководства
    - Определяет возможности имеющихся средств сбора данных, выявляет новые возможности сбора данных
    - Разрабатывает и распространяет планы сбора данных
    - Контролирует выполнение поставленных задач по сбору данных для обеспечения эффективного выполнения плана
  - **Системный аналитик, формирующий требования к сбору данных**
    - Оценивает работу по сбору данных и разрабатывает стратегии рациональной постановки задания, используя доступные источники и методы для улучшения сбора данных
    - Разрабатывает, обрабатывает, подтверждает и координирует задания по сбору данных
    - Оценивает эффективность средств сбора данных и результаты мероприятий по сбору данных
- **Планирование реализации мероприятий в области ИБ**
  - **Специалист по планированию подготовки киберналитики**
    - Разрабатывает подробные планы подготовки аналитических материалов, необходимых для мероприятий по кибербезопасности
    - Сотрудничает со специалистами по планированию мероприятий кибербезопасности для определения, подтверждения и постановки заданий по сбору и анализу данных
    - Участвует в выборе, подтверждении и синхронизации целевых объектов, а также реализации мероприятий по кибербезопасности
    - Синхронизирует действия по подготовке аналитических материалов, чтобы способствовать достижению целей организации в киберпространстве
  - **Руководитель проектов по реализации мероприятий в области ИБ**
    - Разрабатывает подробные планы проведения или поддержки мероприятий по кибербезопасности в сотрудничестве с другими специалистами по планированию, операторами и (или) аналитиками
    - Участвует в выборе, подтверждении и синхронизации целевых объектов, обеспечивает интеграцию в ходе мероприятий по кибербезопасности
  - **Специалист по интеграции с партнерами**
    - Развивает сотрудничество с партнерами из других организаций и государств, с которыми выполняется совместные мероприятия по кибербезопасности
    - Помогает интегрировать команды партнеров: консультирует, предоставляет ресурсы и организует сотрудничество при разработке методических рекомендаций, предоставляет организационную поддержку для успешного проведения совместных мероприятий по кибербезопасности
- **Создание и поддержка базы знаний по расследованию киберинцидентов**
  - **Специалист по базам знаний о киберинцидентах**
    - Осуществляет доступ к целевым системам и эксплуатацию уязвимостей, использует геолокацию для обнаружения местонахождения и отслеживания целевых объектов
    - Осуществляет перемещение в сети, проводит тактический криминалистический анализ, а также по расследованию выполняет задания в целевых сетях

Расследование компьютерных инцидентов

- **Цифровая криминалистика**
  - **Специалист по сбору цифровых данных**
    - Анализирует цифровые доказательства и расследует инциденты кибербезопасности для получения полезной информации с целью снизить уязвимость систем и сетей
  - **Аналитик данных цифровой криминалистики**
    - Проводит детальные расследования компьютерных преступлений, устанавливая документальные или вещественные доказательства, включая цифровые носители и журналы событий, связанные с инцидентами киберпреступления
- **Расследование компьютерных инцидентов**
  - **Специалист по расследованию компьютерных инцидентов**
  - **Следователь по компьютерным инцидентам**
    - Выявляет, собирает, изучает и сохраняет доказательства, используя предписанные методы анализа и расследования, закрепленные в документации