

КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ОРГАНИЗАЦИЙ

ПОДГОТОВКА СПЕЦИАЛИСТОВ

ОСНОВНЫЕ ПОДХОДЫ К ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

- Расширьте способы подбора кадров.**
 - Поддерживает ли ваша организация отношения с университетами и техническими колледжами?
 - Предлагаете ли вы стажировку и обучение в области кибербезопасности?
- Соотнесите имеющиеся способы подбора кадров с открытыми вакансиями.**
 - Эффективно ли ваш отдел кадров представляет требуемые навыки в публикуемых должностных обязанностях?
- Организируйте переобучение сотрудников в специалистов по кибербезопасности.**
 - Могут ли сотрудники переобучиться на специалистов по кибербезопасности в вашей организации?
- Уменьшайте потребность в специалистах по кибербезопасности посредством технологических инноваций.**
 - Есть ли у вас соглашения со сторонними поставщиками услуг о предоставлении резервных ресурсов в случае экстренной необходимости?
- Стимулируйте ваших сотрудников.**
 - Инвестирует ли ваша организация в талантливых специалистов?
 - Предоставляет ли ваша организация возможности для карьерного роста в области кибербезопасности?

ОПРЕДЕЛЕНИЕ ПОТРЕБНОСТЕЙ

- Определите ваши требования по нагрузке.**
 - Оцените сложность выполняемых операций и скорость, с которой они должны выполняться.
 - Оцените необходимость увеличения количества сотрудников и внедрения более продвинутых технологий для снижения вариантов атаки.
- Определите требования, предъявляемые к сотрудникам.**
 - Оцените компетентность, гибкость и скорость мышления специалистов по кибербезопасности в вашей организации.
 - Определите идеальную иерархию штатных должностей и сферы, в которых предпочтение должно отдаваться многофункциональности.
- Определите требуемые знания, навыки, способности и области компетентности для специалистов по кибербезопасности на основе тех рабочих функций, которые они должны выполнять в организации.**
- Определите слабые стороны специалистов по кибербезопасности, уже работающих в вашей организации.**
 - Используйте существующие инструменты, такие как модель NICE, для проведения внутренней оценки ролей и обязанностей.

УЛУЧШЕНИЕ НАБОРА НОВЫХ СОТРУДНИКОВ

- Улучшайте объявления о вакансиях, четко указывая должностные обязанности, согласованные внутри вашей организации.
 - Используйте существующие инструменты, такие как модель NICE, чтобы выделить релевантные наборы навыков.
- Собирайте данные о найме в процессе приема заявлений.
 - Систематизируйте сбор данных и обменивайтесь ими в компании для согласованного подбора и улучшения поиска кадров.
 - Периодически оценивайте данные по найму для выявления недочетов в охвате.
- При оценке потенциала кандидата исходите из нескольких показателей.
 - Рассмотрите возможность систематизированной оценки при найме.
 - Принимайте во внимание наличие дипломов, сертификатов и опыта работы в конкретной сфере.
 - Принимайте решение о найме на основании нескольких показателей.

ДОПОЛНИТЕЛЬНОЕ ВНУТРЕННЕЕ ОБУЧЕНИЕ И КАРЬЕРНЫЙ РОСТ

- Составьте планы карьерного роста и обозначьте возможные пути развития для специалистов по кибербезопасности.
- Определите направления переобучения и переориентирования сотрудников на должности по кибербезопасности в вашей организации.
 - Продумайте альтернативные способы привлечения сотрудников в сферу кибербезопасности, исходя из их интересов и возможностей.
 - Расширяйте программы повышения квалификации и переобучения, а также стимулируйте переводы на другие должности внутри вашей организации.
- Поощряйте обучение и повышение квалификации как внутри вашей организации, так и в других учебных центрах.
 - Предоставьте возможности для дальнейшего обучения и профессиональной аттестации.
- Отслеживайте данные по оттоку и притоку кадров.
 - Регулярно оценивайте данные по оттоку и притоку кадров, чтобы определить, отвечают ли программы требованиям сотрудников.



CarnegieEndowment.org

