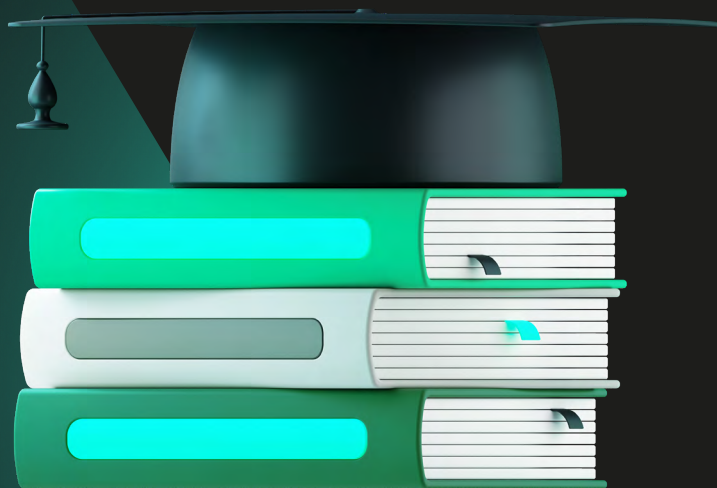




Эффективная стратегия адаптации новых сотрудников и наставничества в командах SOC

Автор статьи – **Ренат Гимадиев, эксперт по решениям для центров кибербезопасности**. Он рассматривает системный подход к адаптации новых сотрудников и наставничеству в современных центрах мониторинга и реагирования (SOC) как критически важный аспект внутреннего планирования, который сокращает сроки подготовки специалиста к самостоятельной работе и способствует снижению рисков выгорания и текучести кадров.

Опираясь на практический опыт, автор предлагает элементы эффективной стратегии, которые помогут новым сотрудникам быстро стать продуктивными членами команды:



структурированные модели адаптации (например, планы на 30–60–90 дней, предусматривающие сбалансированный подход к теории и практике)



наставничество с четким распределением ролей и обязанностей (наставник, бадди, руководитель, стажер)



практико-ориентированные техники передачи знаний, в том числе наблюдение за работой наставника, практика под руководством специалиста, системная обратная связь



KPI (ключевые показатели эффективности, например срок перехода к самостоятельной работе, частотность ошибок по результатам QA, оценка наставника)

Стратегии, использующие эти компоненты, обеспечивают системное развитие уверенных практических навыков у новых аналитиков, повышая эффективность процессов обнаружения и реагирования и укрепляя устойчивость компании к киберугрозам.

Почему адаптация и наставничество важны

В SOC люди являются самым важным активом. Передовые инструменты и четко структурированные процессы играют немалую роль в обнаружении, расследовании и устранении инцидентов, но их эффективность напрямую зависит от профессионализма сотрудников.

Для новичка первые несколько недель в SOC обычно бывают решающими. Без четкого плана адаптации и в отсутствие поддержки со стороны коллег начинающие аналитики могут не справиться с нагрузкой, что негативно скажется на их результатах, снизит мотивацию и повысит риск ухода из компании. Без структурированной системы наставничества знания не усваиваются должным образом, что отрицательно влияет на качество расследований, снижает скорость реагирования и приводит к пропуску критических инцидентов.

Это подтверждают результаты исследования трудовых ресурсов в сфере кибербезопасности, проведенного командой ISC в 2023 году: более **20%** аналитиков SOC испытывают сильный стресс и выгорание, многие из них увольняются, не проработав в компании и двух лет. Исследования также показывают, что без четкого плана адаптации аналитику обычно требуется от шести до девяти месяцев для перехода к полностью самостоятельной работе. И напротив, компании, которые внедряют структурированные программы наставничества, в среднем удерживают до 30% больше специалистов. На практике такой подход может предусматривать сопровождение каждого нового сотрудника наставником при проведении первых расследований.

Эффективные программы адаптации и наставничества предлагают структурированный подход и обеспечивают постоянную поддержку для новых сотрудников, помогая им достичь ясности во всех рабочих вопросах. Это способствует быстрому росту продуктивности новичков, повышает готовность команды к эффективной борьбе со сложными инцидентами и снижает текучесть кадров. Такие программы также ориентированы на непрерывный процесс обучения, что гораздо эффективнее разового вводного курса.

Четко определенные роли

Для успешной реализации программы адаптации и наставничества важно четко распределить роли. Организационная структура SOC может быть неодинакова в разных компаниях, однако рекомендуется распределить среди сотрудников следующие роли:

1

Руководитель (глава SOC или директор по ИБ): осуществляет контроль за реализацией программы адаптации и наставничества, пересматривает ее при изменении бизнес-целей и нормативных требований и оценивает прогресс.

2

Наставник (старший аналитик): знакомит нового сотрудника с рабочими процессами, инструментами и корпоративной культурой, регулярно предоставляет обратную связь, делится практическим опытом.

3

Бадди (дежурный аналитик): помогает решать повседневные вопросы, связанные с рабочими процессами и инструментами.

4

Стажер (новый сотрудник): активно осваивает новые навыки, запрашивает обратную связь, фиксирует накопленный опыт и постепенно расширяет зону ответственности.

Разработка плана адаптации

Тщательно продуманный план адаптации обеспечивает постепенное формирование у новых сотрудников уверенных профессиональных навыков без перегрузки рутинными задачами и сложными инцидентами.

План на 30-60-90 дней – это популярная и проверенная модель со сбалансированным подходом к теории и практике на время испытательного срока. Вот ее краткое описание.

Первые 30 дней – знакомство и наблюдение

Знакомство с задачами SOC, структурой команды и иерархией; освоение базовых инструментов; наблюдение за работой наставника; первичное взаимодействие с другими отделами, например IT, юридическим и так далее. На этом этапе новые сотрудники могут принимать участие в практических учениях или игровых мини-тренингах, что позволит им сформировать рабочие навыки без стресса, вызываемого обработкой реальных инцидентов.

Дни 31-60 – практика под руководством специалиста

Обработка оповещений с низким уровнем критичности под руководством опытного специалиста, выполнение стандартных запросов, создание заявок и участие в подготовке статей для базы знаний. На данном этапе следует также предоставить стажерам возможность удаленного наблюдения за работой опытных сотрудников и изучения других аспектов кибербезопасности (например, краткосрочную практику в роли специалиста по активному поиску угроз или криминалистическому анализу) для получения дополнительных контекстных знаний.

Дни 61-90 – самостоятельная работа

Первичная классификация инцидентов, расследования с последующим анализом со стороны наставника и первые шаги в роли наставника для новичков. На этом этапе аналитики уже должны адаптироваться к повседневному режиму работы, однако темпы развития индивидуальны – кому-то достаточно 60 дней, а кому-то потребуется 120. Самое главное – еженедельно проводить сеансы обратной связи между стажером, наставником и руководителем SOC, чтобы обеспечить единое понимание целей и снизить риски упустить что-то важное.

В заключение отметим, что процесс адаптации специалистов SOC может отличаться: все зависит от начальных знаний и опыта работы с продуктами и сервисами ИБ, однако при системном подходе и должном внимании необходимые компетенции формируются достаточно быстро.

Разработка эффективной программы наставничества

Наставничество – структурированный процесс с четко определенными этапами и измеряемыми результатами. Обучение выстраивается следующим образом:

Наблюдение → совместная работа → самостоятельная работа: сначала стажер повторяет действия наставника, затем стажер и наставник вместе решают рабочие задачи, и, наконец, стажер самостоятельно расследует инциденты с минимальным вмешательством.

Регулярное взаимодействие: еженедельные встречи 1:1, ежедневные брифинги перед началом рабочей смены, формальная оценка навыков, разбор текущих сложностей и прочее.

Эффективные подходы: ограниченное число стажеров на одного наставника, например не более двух; документальное оформление обратной связи; фиксация ключевых результатов; систематический сбор обратной связи.

Показатель	Определение	Целевое значение	Почему это важно
Срок перехода к самостоятельной работе	Количество дней с момента трудоустройства до самостоятельной обработки простых инцидентов	60-90 дней	Снижение нагрузки на команду
Частотность ошибок по результатам QA	Доля заявок об инцидентах, оформленных с отклонениями от стандартов	< 5% через 90 дней	Поддержание качества работы и соблюдение нормативных требований
Уровень удержания специалистов	Доля сотрудников, которые продолжают работать в компании по истечении 6-12 месяцев с момента трудоустройства	> 85%	Снижение затрат на подбор и обучение персонала
Уровень удовлетворенности наставника/стажера	Оценка по результатам структурированных опросов	$\geq 4/5$	Вовлеченность сотрудников и эффективность программы
Выполнение сценариев	Доля корректно выполненных этапов работы	> 95%	Согласованность действий и готовность к аудиту

Эффективные подходы: обучение работе с инструментами с одновременным объяснением процессов; поддержание актуальности и регулярное обновление базы знаний; признание и поощрение лучших наставников; использование смешанных форматов обучения.

Распространенные ошибки: высокая нагрузка на наставников; фокус исключительно на профессиональных навыках; нерегулярная обратная связь от стажеров; подход к адаптации как к разовому мероприятию, а не как к непрерывному процессу.



Заключение

Адаптация и наставничество – это гораздо больше, чем формальные HR-процедуры. Скорее, это стратегические процессы, которые напрямую влияют на эффективность SOC и качество обслуживания. Структурированная программа поможет аналитикам быстрее стать полноценными членами команды и предотвратит выгорание. Компании не придется постоянно искать новых сотрудников и нести связанные с этим расходы.

Помимо повышения продуктивности, такие программы позволяют улучшить качество обнаружения и реагирования. Аналитики, завершившие эффективную программу адаптации, увереннее работают с инцидентами, точнее следуют сценариям реагирования и постоянно расширяют базу знаний SOC. Без системы наставничества критически важные знания, например о тонкостях работы с SIEM, остаются достоянием лишь одного аналитика и зачастую покидают компанию вместе с ним.

Наставничество позволяет достичь важных для компании и измеримых результатов: сократить среднее время обнаружения и реагирования, повысить готовность к аудиту и обеспечить соблюдение нормативных требований. Вкладывая средства в развитие сотрудников, руководители смогут сформировать зрелую культуру, где аналитики SOC чувствуют свою значимость, поддержку со стороны коллег и мотивацию к дальнейшему развитию.

В конце концов, даже лучшие инструменты могут оказаться бесполезными, если сотрудники не умеют ими пользоваться. Эффективная программа адаптации и наставничества позволяет сформировать команду, которая будет мгновенно реагировать на каждую новую угрозу. Никто не знает, когда это случится, поэтому сотрудники должны постоянно совершенствовать свои навыки и быть готовыми отразить атаку в любой момент.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности и защиты конфиденциальности данных с 1997 года. Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важных инфраструктур, государственных учреждений и рядовых пользователей, защищая миллиарды устройств от новейших угроз и целевых атак. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты рабочих мест, а также ряд специализированных решений и сервисов для борьбы с комплексными и постоянно эволюционирующими киберугрозами, в том числе кибериммунные системы. Наши технологии обеспечивают защиту самых важных аспектов бизнеса более 200 тысяч корпоративных клиентов. Подробнее см. на сайте www.kaspersky.ru.