автоматически генерируемых журналов событий. В рассматриваемом подходе задачей группы центра оперативного реагирования на инциденты в сфере информационной безопасности является ручной анализ данных из различных источников и принятие решения для какого-либо действия в зависимости от уровня критичности.

Ханипоты не могут полностью заменить такие средства защиты информации, как средства обнаружения вторжений или межсетевые экраны. Однако ханипоты являются прекрасным средством для изучения инструментария и методологии злоумышленников и улучшения систем защиты информации с помощью полученной информации. Помимо этого, благодаря возможности использования человеческих способностей для принятия решении о критичности события, ханипоты могут стать прекрасным дополнением функционирования центра оперативного реагирования на инциденты в сфере информационной безопасности (SOC).

Список литературы

1. Rahul Koul, Bakal J.W. Modern attack detection using intelligent honeypot // International research journal of engineering and technology. 2017. № 4. P. 2866–2869.

2. Назначение технологии Honeypot. [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/275420.php?R=1 (дата обращения: 02.05.2019).

ОСОБЕННОСТИ ПОДГОТОВКИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

М.В. Губич

Развитие информационного общества обусловило рост количества информации в электронном виде, подлежащей защите, и регистрируемых киберпреступлений, что в свою очередь повлекло необходимость подготовки квалифицированных кадров, обученных общим вопросам обеспечения информационной безопасности, и отдельной категории сотрудников, способных эффективно противодействовать преступлениям в сфере высоких технологий.

В связи с этим одной из основных целей профессиональной подготовки специалиста юридического профиля для правоохранительной сферы становится непрерывная компьютерная подготовка, в рамках которой должна быть сформирована готовность к использованию информационно-коммуникационных технологий (ИКТ), являющаяся базовой основой для развития компетенций в области информационной безопасности. К составляющим готовности к использованию ИКТ мы относим теоретические знания, технологические умения, навыки и профессиональные качества, личностные и мотивационные качества.

Соответственно, концепция формирования готовности к использованию ИКТ, на наш взгляд, должна быть основана на принципах обучения, способствующих овладению умениями решать профессиональные задачи и проблемы правоохранительной сферы на базовом (на уровне пользователя на основе выполнения установленных требований по информационной безопасности), углубленном (на уровне продвинутого пользователя, осуществляющего мероприятия по обеспечению информационной безопасности собственного рабочего места пользователя на основе выполнения требований технических и иных нормативных правовых актов) и специальном уровнях (умение решать служебные задачи на основе внедрения в служебную деятельность новых ИКТ, разработки собственных систем и средств обеспечения информационной безопасности рабочих мест пользователей ИКТ организации, а также противодействовать компьютерной преступности).

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ПОМОЩЬЮ ПОИСКОВОЙ СИСТЕМЫ SHODAN

Ш.Р. Давлатов

Shodan – это ведущая поисковая система по Интернету вещей, существующая уже более семи лет. В отличие от популярных поисковых движков (Google, Yandex, Bing и др.), которые ищут в сети информацию из обычных сайтов, система Shodan работает с теневыми каналами