ятельствами наказывается от 25 до 30 лет лишения свободы: 1) когда присутствуют два или более обстоятельства из предыдущей статьи; 2) удушение, пожар, взрыв или отравление; 3) избиение, увечье или расчленение трупа; 4) в присутствии ребенка или подростка; 5) жертва является ребенком или подростком; 6) уязвимое лицо.

В целом в Никарагуа происходит значительная модернизация законодательства, связанная с юрисдикционными аспектами, такими как вступление в силу пяти новых кодексов – Уголовно-процессуального кодекса, Уголовного кодекса, Трудового кодекса, Семейного кодекса, Гражданского процессуального кодекса. УПК впервые в истории вводит в страну такие методы судопроизводства, как устность, открытость и непосредственность, направленные на разрешение конфликтов и эффективное и быстрое осуществление правосудия. Эти законы были предложены в качестве инициативы Верховного суда и разработаны другими ветвями государственной власти, участвующими в законодательном процессе страны, поскольку они отражают волю никарагуанцев строить, укреплять и продвигаться к лучшей демократии через уважение к законам и обеспечение эффективной защиты прав и благ граждан, так как они принимают на себя национальный запрос и надежду жить в гармонии, безопасности, мире и прогрессе, посредством защиты законов и принимая в качестве инструмента правильное и корректное выполнение функций судебных органов.

Звягин Д.С.,

кандидат технических наук
Воронежский институт МВД России

Соблюдение мер информационной безопасности при осуществлении кибербразведки

В условиях усиления киберугроз организации все чаще прибегают к освещенной в нормативных документах практике кибербразведки (cyber threat intelligence, CTI). Однако сами по себе активная сборка, анализ и распространение разведданных несет новые риски утечки конфиденциальной информации и нарушения законодательства. В работе кратко систематизированы принципы и технические решения, позволяющие одновременно выполнять задачи CTI и соблюдать требования информационной безопасности (ИБ).

Кибербразведка рассматривается как непрерывный процесс выявления индикаторов компрометации, атрибутов атакующих и их тактик, техник и процедур. Стандарты ISO/IEC 27001 и ГОСТ Р 57580-2017 предписывают организациям внедрять процессы мониторинга и обмена данными об угрозах.

При этом неочевидным остается вопрос правомерной обработки сведений, относящихся к государственной тайне, коммерческим секретам и персональным данным[1].

Основные законодательные акты России (федеральные законы «О персональных данных», «Об информации…») устанавливают требования к сбору и трансграничной передаче сведений. В контексте CTI особое значение приобретают:

– согласие субъектов – при обработке PII, полученной из открытых источников OSINT;

– критическая ИКТ-инфраструктура – запрет на вывод журналов из сегментов КИИ без контроля[2].

– экспорт криптосредств – шифрованные каналы передачи разведданных могут подпадать под ограничения ФСТЭК/ФСБ.

Организационные меры

– политика «need-to-know» для команд SOC и аналитиков: разграничение доступа к данным о внутренних инцидентах;

– юридическая верификация источников: контракты с внешними провайдерами CTI должны включать классификацию данных и ответственность за соблюдение ПДн;

– процедура sanitization перед публикацией отчетов: удаление осовремененных индикаторов, которые могут выдать внутреннюю инфраструктуру.

Технические меры

– двухконтурная архитектура CTI-платформы:

внутренний контур (TAXII-сервер, MISP) хранит сырые данные;

внешний контур предоставляет агрегированные и анонимизированные артефакты партнерам;

– Label-based access control (TLP, FIRST CSIRT) с автоматическим присвоением меток STIX 2.1;

–Homomorphic hashing при сопоставлении IOC, что исключает передачу исходных значений хэшей паролей;

– Trusted execution environments (TEE) для обработки кодов эксплойтов без раскрытия их содержимого аналитикам.

Соблюдение мер ИБ не препятствует эффективности кибербразведки, если процессы выстроены по принципу «секьюрити-бай-дизайн»: юридическая экспертиза, адаптированные модели разграничения доступа и современные криптографические подходы позволяют безопасно обмениваться CTI-данными внутри отраслевых центров.

[1] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ.

[2] О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ.