УДК 355.23:004.056.5:004.89:343.9:378

Ф.Н. Супрун, преп. кафедры связи;
С.В. Сидоров, ст. преп. кафедры связи
(БГУИР, г. Минск)

АКТУАЛЬНОСТЬ ОБУЧЕНИЯ ОСНОВАМ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ (ФОРЕНЗИКИ) В СИСТЕМЕ ВЫСШЕГО ВОЕННОГО ОБРАЗОВАНИЯ

Современная геополитическая обстановка характеризуется смещением акцентов от традиционных методов ведения боевых действий в сторону гибридных конфликтов, где информационное противоборство занимает доминирующую позицию. В этих условиях информационно-коммуникационная инфраструктура Вооруженных Сил становится приоритетной целью для деструктивного воздействия. Следовательно, система военного образования должна гибко реагировать на возникающие угрозы, адаптируя учебные программы под реалии киберпространства.

Одним из наиболее перспективных направлений совершенствования подготовки военных специалистов в области связи и защиты информации является внедрение в образовательный процесс дисциплины «Компьютерная криминалистика» (цифровая форензика).

На сегодняшний день анализ учебных планов профильных специальностей в высших военных учебных заведениях показывает, что основной упор делается на технологии обеспечения безопасности (prevention and protection). Курсанты детально изучают методы криптографической защиты, настройки межсетевых экранов, администрирование защищенных операционных систем (в частности, на базе ядра Linux) и построение защищенных сетей связи. Безусловно, это фундамент информационной безопасности. Однако данный подход охватывает лишь превентивную сторону вопроса.

Проблема заключается в том, что в реальных условиях стопроцентная защита невозможна. Инциденты информационной безопасности (ИИБ) неизбежны, будь то целенаправленная хакерская атака, инсайдерская деятельность или нарушение правил эксплуатации техники личным составом.

В текущей парадигме обучения выпускник, столкнувшись с фактом компрометации узла связи или сервера, зачастую не обладает компетенциями для проведения квалифицированного расследования. Стандартная реакция администратора – переустановка системы или форматирование носителя, что фактически уничтожает следы вторжения (улики) и делает невозможным установление источника атаки, её вектора и масштаба утечки данных.

Именно здесь возникает насущная потребность в компетенциях цифровой форензики. Внедрение элементов компьютерной криминалистики в систему военного образования позволит решить следующие задачи:

Во-первых, формирование навыков реагирования на инциденты (Incident Response). Будущий офицер должен понимать алгоритм действий при обнаружении несанкционированного доступа. Главным принципом здесь выступает сохранение неизменности доказательств. Обучающиеся должны четко усвоить разницу между работой с «живой» системой (Live Forensics) и анализом остановленных систем (Dead Forensics). Например, понимание того, что простое выключение питания сервера приведет к потере содержимого оперативной памяти, где могут храниться ключи шифрования или следы активных сетевых соединений злоумышленника, является критически важным.

Во-вторых, углубленное изучение архитектуры операционных систем и сетей. Форензика требует не поверхностного, а глубинного знания технологий. При изучении данной дисциплины курсанты переходят от пользовательского уровня к экспертному. Рассматривая структуру файловых систем (EXT4, NTFS), механизмы журналирования, принципы выделения памяти и структуру сетевых пакетов, обучающиеся начинают лучше понимать работу техники в целом. Например, практическая отработка создания дампа оперативной памяти или побитовой копии жесткого диска (с использованием утилиты dd) закрепляет знания о физическом устройстве носителей информации.

В-третьих, правовая грамотность и процессуальная точность. Военный специалист должен понимать юридические последствия своих действий. В условиях, когда кибератаки могут квалифицироваться как акты агрессии или уголовные преступления, корректный сбор и фиксация цифровых доказательств становятся обязательным условием для привлечения виновных к ответственности. Это требует введения в курс обучения тем, связанных с цепочкой обеспечения сохранности доказательств (chain of custody) и документированием процесса расследования.

Анализируя тренды развития военного образования, можно предложить следующую модель интеграции форензики в учебный процесс:

Модернизация лабораторной базы. Создание киберполигонов (Cyber Ranges), эмулирующих типовую информационную инфраструктуру воинской части. Это позволит проводить учения типа «Red Teaming / Blue Teaming» (атака/защита), где одна группа курсантов реализует вектор атаки, а вторая – проводит расследование инцидента,

анализирует логи, сетевой трафик (pcap-файлы) и восстанавливает хронологию событий.

Практико-ориентированный подход. Включение в учебные вопросы тем по анализу артефактов ОС Linux, так как данная платформа является базовой для многих систем специального назначения. Курсанты должны уметь анализировать журналы системных событий, историю командной оболочки (bash history), конфигурационные файлы демонов (SSH, httpd) и временные метки файлов.

Междисциплинарные связи. Элементы форензики должны пронизывать и другие дисциплины. На занятиях по сетевым технологиям целесообразно рассматривать не только настройку маршрутизации, но и анализ сетевых дампов для выявления аномалий. На занятиях по программированию – основы реверс-инжиниринга вредоносного кода.

Детализируя содержание предлагаемой дисциплины, необходимо отметить, что специфика подготовки военных инженеров требует смещения фокуса с общих вопросов компьютерной безопасности на углубленный анализ системного программного обеспечения. В частности, учитывая широкое распространение операционных систем на базе ядра Linux в комплексах управления войсками и оружием, программа обучения должна включать детальный разбор архитектурных особенностей данной ОС.

Курсанты должны на практике освоить методику сбора цифровых доказательств в среде Linux, которая существенно отличается от работы в среде Windows. Ключевыми компетенциями здесь являются: понимание концепции inode (индексных дескрипторов) и файловых меток времени (MAC-times: Modification, Access, Change). Зачастую злоумышленники, пытаясь скрыть свое присутствие, изменяют содержимое файлов, но забывают скорректировать метаданные файловой системы. Умение анализировать несоответствия во временных метках позволяет офицеру выявить факт подлога информации или подмены исполняемых файлов.

С методической точки зрения, реализация такой подготовки невозможна без широкого применения технологий виртуализации. Традиционные методы обучения «на железе» не позволяют в полной мере реализовать деструктивные сценарии без риска повреждения реального оборудования учебно-материальной базы.

Внедрение виртуальных полигонов позволяет каждому курсанту работать в изолированной среде («песочнице»). Преподаватель получает возможность мгновенно развертывать сценарии инцидентов (например, заражение системы вирусом-шифровальщиком или внедрение rootkit) с помощью системы снимков состояния (snapshots). Это

дает возможность обучающимся совершать ошибки, анализировать их последствия и возвращать систему в исходное состояние для повторной отработки, что существенно интенсифицирует процесс обучения.

Также перспективным направлением является внедрение элементов соревновательной механики (CTF – Capture The Flag) в итоговый контроль знаний. Проведение внутривузовских киберучений, где одна группа курсантов защищает периметр и расследует инциденты, а другая пытается реализовать вектор атаки, максимально приближает учебный процесс к боевым условиям. Такой подход формирует не только технические навыки, но и стрессоустойчивость, умение работать в команде и принимать решения в условиях дефицита времени и неполноты информации.

Таким образом, актуальность обучения основам компьютерной криминалистики обусловлена необходимостью перехода от пассивной защиты информации к активному противодействию киберугрозам. Специалист, владеющий методами форензики, способен не просто эксплуатировать технику, но и обеспечивать её живучесть, выявлять скрытые угрозы и предоставлять командованию объективную информацию о причинах и последствиях киберинцидентов. Это качественно новый уровень подготовки, соответствующий требованиям современной высокотехнологичной войны.

Внедрение данных компетенций в образовательные стандарты позволит выпускать офицеров, способных эффективно действовать в условиях агрессивной информационной среды, минимизируя ущерб от действий противника и обеспечивая непрерывность управления войсками.

ЛИТЕРАТУРА

1. Федотов, Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М.: Юридический мир, 2007. – 432 с.

2. Скабцов, Н. Аудит безопасности информационных систем / Н. Скабцов. – СПб.: Питер, 2018. – 272 с.

3. Основы компьютерной криминалистики: учебное пособие / В. А. Минаев [и др.]. – М.: Маросейка, 2010. – 250 с.

4. Проблема подготовки кадров в области информационной безопасности для Вооруженных Сил: сб. науч. ст. / под ред. А. Г. Иванова. – Минск: ВА РБ, 2023. – С. 45–49.