ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
Московский институт электроники и математики им. А.Н.Тихонова

Дополнительная активность. Основы цифровой форензики.

По направлению 10.04.01 – «Информационная безопасность»

Проверил:
преп. Сорокин А. В.
Подпись
_____
Выполнил:
Новиков В. С. МКБ 241
Подпись
_____

Москва 2025

Дополнительные активности по курсу «Основы цифровой форензики»
подготовил студент Новиков В. С. Группа МКБ 241 (2025г.)

№	Формат	Краткое описание	Инструменты	Объём / балл
1	Лабораторная работа «Mobile Forensics»	Разбор образа памяти Android-смартфона: извлечение SMS, WhatsApp, геолокаций. Навык — логическая/физическая экстракция, формирование отчёта о доказательствах.	MOBILedit (demo), AFLogical OSE или Android Backup Extractor.	4 акад. ч; 0,2 б
2	Практикум «Timeline Construction»	Построение единой временной шкалы (логи, MFT, USN Journal, web-history) и корреляция с инцидентом.	Plaso/log2timeline, Timesketch	4 ч; 0,2 б
3	Мини-CTF «Memory + Disk Triad»	6-8 флагов: implant в RAM, восстановление удалённого файла, поиск persistence-механизма.	FTK Imager, Volatility, Autopsy	1 нед.; до 0,4 б
4	Table-top «Incident Response Drill»	Командная отработка плана реагирования: утечка, инсайдер, DDoS. Подготовка chain of custody.	Карточки сценариев, шаблон IR-плана	2 ч; 0,1 б
5	Семинар «Судебная практика РФ»	Анализ реальных решений судов с цифровыми доказательствами; разбор ошибок экспертов.	Консультант+, ГАС Правосудие	2 ч; 0,1 б
6	Workshop «Cloud & Log Forensics»	Разбор логов AWS CloudTrail/Azure AD, импорт в ELK, дашборды.	AWS Free Tier, Kibana (playground)	4 ч; 0,2 б

7	Домашнее исследование «Browser Artifacts »	Извлечение history, cookies, saved-passwords из профиля Chrome/Firefox, отчёт экспертного типа.	browser-history-capturer, DB Browser for SQLite	1 нед.; 0,2 б
8	Гостевая лекция + дебриф	Выступление практикующего эксперта (СКР, CERT, PT). Студенты готовят вопросы и резюме уроков.	Zoom/аудитория	1,5 ч; 0,05 б
9	Ролевой суд («Модельный процесс»)	Роли: эксперт, адвокат, прокурор, судья. Защита выводов по флеш-образу.	Подготовленный образ, регламент суда	2 ч; 0,15 б

Максимальный суммарный бонус за дополнительные активности — 0,2 балла (студент выбирает одну-две активности).

Как вписывается в текущую структуру курса:

- лекции 1–2 (понятия, память) → активности 2, 3, 7;
- лекция 4 (сеть) → активность 6 и часть CTF;
- домашние задания уже охватывают RAM, disk, pcap; новые задания добавляют mobile, cloud, timeline, legal aspect и практику публичного представления выводов.

Организация и оценивание:

- каждая активность—неблокирующий «доп. элемент» (*О доп.*) из презентации лекции 1.
- максимум зачтённых дополнительных баллов — 0,2 (как и для инициативы). Студент может выбрать одну-две активности на выбор.
- мини-CTF может проходить заочно (сервер с флагами) и даёт сразу полный бонус 0,2 балла.
- для каждой активности хорошо бы приложить мини-гайд (PDF / MD) с инструкциями — снизит нагрузку на преподавателя во время лабораторных.

Необходимые ресурсы кафедры:

- USB-диски с подготовленными образами, VPN к облачному стенду.

Эти активности расширят спектр компетенций: от классических RAM/Disk к mobile, cloud, OSINT и судебной практике — и дадут студентам возможность заработать «инициативные» баллы живыми, практически полезными задачами.