GROUP-IB

EDUCATION | EU, APAC

LEADING-EDGE CYBERSECURITY EDUCATION PROGRAMS

EDUCATION@GROUP-IB.COM

The cyber professions of the future

Develop the cybersecurity competencies you need to master in order to operate effectively and protect your company from cyber threats

Why choose Group-IB's training courses?

World-class team of active experts

Courses are conducted by certified specialists who actively respond to and investigate high-profile cybercrimes worldwide. This ensures that course materials comprise relevant, first-hand cybersecurity insights.

Continuously updated program

Courses are conducted by certified specialists who actively respond to and investigate high-profile cybercrimes worldwide. This ensures that course materials comprise relevant, first-hand cybersecurity insights.

Stimulating practical training

Each course comprises practical exercises based on real-life cases. Such exercises make up 70% of the course to ensure students truly understand how to apply knowledge learned.

Full-spectrum support for IS development

Group-IB's role-based learning model provides a balance of skills and tools needed to build an effective information security team and ensure security in any company.

11 modules
Trainings for technical specialists

1 workshop
Cybersecurity awareness

1 interactive game
Incident Response simulation game

Cyber Security Hero Path

- Blue Team Analyst
- Threat Intelligence Analyst

SOC Analyst

- Incident Responder
- Windows DFIR Analyst
- Linux DFIR Analyst
- Network Forensics Analyst
- Threat Intelligence Analyst
- Malware Analyst

Incident Responder

- Blue Team Analyst
- Threat Intelligence Analyst
- Threat Hunter

Threat Hunter

- Threat Intelligence Analyst
- Malware Analyst

Malware Analyst

Threat Intelligence Analyst

TI Analyst

- Threat Intelligence Analyst
- Cyber Investigator

Cyber Investigator

Penetration Tester

Penetration Tester

Format:

Online | Offline (By request)

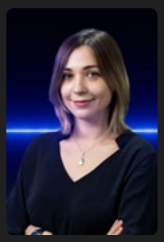
Collective groups | Corporate groups

Group-IB trainers:

Anastasia Barinova,

Head of Education

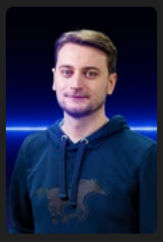
Anastasia conducts digital forensics research, regularly participates in conferences, and develops training courses on digital forensics, incident response, threat hunting, and threat information collection and analysis.She has held more than 60 training sessions across four continents and teaches original courses on digital forensics and fighting cybercrime at the Higher School of Economics, MGIMO, Moscow Institute of Physics and Technology, and Bauman Moscow State Technical University.



Svetlana Ostrovskaya,

Principal Incident Response and Digital Forensics Analyst

Besides active involvement in incident response engagements, Svetlana has co-authored articles on information security and computer forensics as well as a book dedicated to practical memory forensics. In addition, Svetlana develops and updates courses on advanced digital forensics, monitoring and incident response, attends professional conferences, regularly conducts trainings and master classes all over the world.



Roman Rezvukhin,

Head of Malware Analysis and Threat Hunting Team

Roman has been working in malware analysis and reverse engineering for more than six years and regularly takes part in complex incident response operations worldwide.

Roman reverse-engineers tools and malware used in complex attacks and develops utilities that automate incident response and malware analysis processes.

Anatoly Tykushin,

Head of Digital Forensics Laboratory

Anatoly has conducted a research study on digital forensics, the findings of which have been presented at conferences and used in real incident response cases. He teaches digital forensics at Innopolis and Skolkovo Universities, both of which are leading Russian higher education institutions in IT, science, and technology.

Anatoly regularly takes part in complex incident response operations, conducts digital forensic investigations, develops methodologies, and assesses organizations' incident response readiness.

Group-IB Training Programs

Course title	About	Duration	Target audience	More info
INCIDENT RESPONDER Level: ●●●○	Learn how to stop cyberattacks, prioritize incidents, and mitigate the damage.	3 days 6 h / day	• Incident response enthusiasts • Technical specialists with experience in IS • Information security specialists • SOC/CERT employees	
WINDOWS DFIR ANALYST Level: ●●●●	Learn how to understand forensics acquisition methods, create forensic images and analyze artifacts to reconstruct attacker's techniques.	5 days 6 h / day	• Information security specialists • Technical specialists with experience in IS • Incident responders	
LINUX DFIR ANALYST Level: ●●●○	Practical course on forensics of Linux-based systems during the incident.	2 days 6 h / day	• Information security specialists • Technical specialists with experience in IS • Incident responders	
BLUE TEAM ANALYST Level: ●●○○	Learn how to monitor for IS incidents, detect threats, eliminate false positives, and perform initial incident response.	3 days 6 h / day	• Technical specialists with experience in IS • Information security specialists • SOC/CERT employees	
NETWORK FORENSICS ANALYST Level: ●●○○	Practical course on network forensics for incident response needs.	2 days 6 h / day	• Information security specialists • Incident responders • SOC/CERT analysts • Digital forensics specialists	
CYBER INVESTIGATOR Level: ●●○○	Learn how to interpret data to catch criminals lurking in the dark web and underground.	4 days 6 h / day	• IT specialists with experience in information security • Information security experts • Practicing digital forensics and incident response specialists	
VIDEO COURSE MALWARE ANALYST Level: ●●●●	Learn how to analyze malware found during incident response engagements or forensic analysis of infected objects.	3 week video course	• Incident response professionals • Digital forensics specialists • SOC teams	
THREAT HUNTER Level: ●●●○	Learn how to proactively hunt for hidden, undetectable threats within the organization.	4 days 6 h / day	• Technical specialists with experience in IS • IS experts • Threat hunters	
TI ANALYST Level: ●●○○	Learn how to collect actionable intel and interpret the data for effective incident response and attacker attribution.	2 days 6 h / day	• Technical specialists with experience in IS • Information security specialists • SOC/CERT employees	
ANTI-FRAUD ANALYST Level: ●●○○ For corporate groups only	An introduction to in-session antifraud systems and the types of fraud they are used to counteract.	2 days 6 h / day	• Cyberthreat monitoring specialists • Technical specialists with basic experience in information security • Heads of security and IT departments • Executives in charge of supplementary office channels used by clients	
PENETRATION TESTER Level: ●●○○	Discover the way cybercriminals think and learn how to use various techniques to increase the security of an organization.	3 days 6 h / day	• IS professionals transitioning into penetration testing • System/network administrators/ engineers • SOC/CERT/CSIRT employees • Technical specialists with experience in IS • Information security professionals • Penetration testing enthusiasts	

About Group-IB

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

1,300+ successful investigations	**600+** employees	**550+** enterprise customers	**60** countries
$1 bln saved for companies	**#1*** Incident Response Retainer vendor	**120+** patents and applications	**4** unique Threat Intelligence and Research centers

* According to Cybersecurity Excellence Awards

Global partnerships

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting		• Security Assessment • Penetration Testing	• Red Teaming • Compliance & Consulting
Education & Training		• For technical specialists • For wider audiences	
DFIR	• Incident Response • Incident Response Retainer	• Incident Response Readiness Assessment • Compromise Assessment	• Digital Forensics • eDiscovery
Managed Services		• Managed Detection • Managed Threat Hunting	• Managed Response
High-Tech Crime Investigation		• Cyber Investigation • Investigation Subscription	

GROUP-IB

How to sign up for a course?

Send us a request for an individual consultation on Group-IB training courses

FIGHT AGAINST CYBERCRIME

GROUP-IB.COM
INFO@GROUP-IB.COM

EDUCATION@GROUP-IB.COM