

Приложение 9. Глоссарий

APT-атака	От англ. Advanced Persistent Threat (целевая сложная кибератака). Это целенаправленная, сложная в техническом плане и скрытая кибератака, в рамках которой злоумышленники собирают конфиденциальные данные или наносят значительный ущерб компании или определенному человеку
BEC	От англ. Business Email Compromise (компрометация деловой электронной почты) — вид мошеннической атаки, при которой злоумышленник выдает себя за сотрудника, руководителя или контрагента компании в деловой переписке, чтобы добиться перевода денежных средств, передачи данных или иных действий в ущерб компании
DDoS	От англ. Distributed Denial of Service (распределенная атака типа «отказ в обслуживании»). Атака, при которой множество устройств одновременно направляют поток запросов на сервер, сервис или сеть, чтобы перегрузить их и сделать недоступными для пользователей
DLL Hijacking	От англ. Dynamic Link Library Hijacking (подмена динамической библиотеки) — техника атаки, при которой злоумышленник подменяет или размещает вредоносную DLL-библиотеку так, что легитимная программа загружает ее вместо штатной и выполняет вредоносный код
DPI	От англ. Deep Packet Inspection (глубокий анализ трафика). Технология анализа сетевого трафика, позволяющая исследовать не только заголовки пакетов, но и их содержимое для выявления угроз, фильтрации данных и контроля передачи информации
EDR	От англ. Endpoint Detection and Response (обнаружение и реагирование на угрозы на конечных устройствах). Класс решений информационной безопасности, предназначенных для мониторинга конечных устройств, выявления подозрительной активности, расследования инцидентов и реагирования на них
IoT	От англ. Internet of Things (интернет вещей). Сеть взаимосвязанных физических устройств, оснащенных датчиками, программным обеспечением и средствами связи для обмена данными между собой, с облачными системами и другими цифровыми платформами
LLM	От англ. Large Language Model (большая языковая модель). Модель искусственного интеллекта, обученная на больших массивах текстовых данных и способная понимать и генерировать естественный язык, а также выполнять связанные с текстом задачи
Решения MDR	От англ. Managed Detection and Response (управляемое обнаружение и реагирование). Решения для автоматического обнаружения и анализа инцидентов безопасности в инфраструктуре с помощью телеметрии и передовых технологий машинного обучения

OCR	От англ. Optical Character Recognition (оптическое распознавание символов). Технология преобразования текста на изображениях, сканах или фотографиях в машиночитаемый формат для дальнейшей обработки, хранения и поиска
OT-инфраструктура	От англ. Operational Technology (операционные технологии). Совокупность систем, оборудования и программного обеспечения, которые управляют физическими процессами в промышленности, энергетике, транспорте и на других объектах критической инфраструктуры
POSA-карты	От англ. Point of Sale Activation. Продукт, который активируется в точке продаж
SOC	От англ. Security Operations Center (центр мониторинга и реагирования на инциденты информационной безопасности). Выделенная функция или подразделение, которое в непрерывном режиме отслеживает события информационной безопасности, выявляет угрозы и координирует реагирование на инциденты
TIP	От англ. Threat Intelligence Platform (платформа аналитики киберугроз). Платформа для сбора, обогащения, анализа и использования данных о киберугрозах, включая индикаторы компрометации, сведения о злоумышленниках и их тактиках
Vehicle-to-Everything	От англ. Vehicle-to-Everything (обмен данными транспортного средства со всем окружением). Технология обмена информацией в реальном времени между транспортным средством и другими объектами: автомобилями, дорожной инфраструктурой, пешеходами, сетями и облачными системами
XDR	От англ. Extended Detection and Response (расширенное обнаружение и реагирование). Класс систем информационной безопасности, предназначенных для автоматического проактивного выявления угроз на разных уровнях инфраструктуры, реагирования на них и противодействия сложным атакам
АСУ ТП	Автоматизированная система управления технологическим процессом — Комплекс программных и аппаратных средств, предназначенных для автоматизации, мониторинга и управления технологическими процессами на производстве и в промышленной инфраструктуре
Вайперы	От англ. Wiper malware (вредоносные программы для уничтожения данных). Отдельная разновидность программ-шифровальщиков, цель которых — безвозвратное уничтожение данных, восстановление после такой атаки становится невозможным

Вендор	От англ. Vendor (поставщик, производитель). Компания, которая разрабатывает, производит и (или) поставляет продукты, решения или услуги под собственным брендом
Вирусы, черви, троянцы	Распространенные типы вредоносных программ: вирусы внедряются в файлы и распространяются при их запуске, черви распространяются самостоятельно, трояны маскируются под легитимное программное обеспечение
Киберсталкинг	Систематическое преследование человека, группы лиц или компании, их запугивание и (или) домогательство с использованием интернета и других электронных средств коммуникации. Киберсталкингом могут заниматься как родственники и знакомые жертвы, так и организации и посторонние люди
Кликер-игры	От англ. Clicker games / Idle games (кликер-игры). Жанр цифровых игр, основанный на многократных простых действиях пользователя или автоматическом накоплении игровых ресурсов
Конечные точки, конечные устройства	Физические устройства, подключенные к корпоративной или иной сети и способные обмениваться данными с другими системами: компьютеры, ноутбуки, смартфоны, серверы, виртуальные машины и встроенные устройства
Майнинг	Процесс создания новых блоков информации о совершенных с определенной криптовалютой (например, биткойн) транзакциях и добавления их в блокчейн. Каждый новый блок содержит информацию о транзакциях, произошедших с момента создания предыдущего блока. Цель майнинга — подтверждение транзакций с единицами криптовалюты (токенами) и добавление новых единиц в систему (которые являются прибылью майнеров)

Поколение Z	От англ. Generation Z — поколение людей, родившихся ориентировочно с середины 1990-х до начала 2010-х годов и выросших в условиях широкого распространения цифровых технологий и интернета
Реверс-инжиниринг	От англ. Reverse Engineering — обратная разработка кода. Это процесс анализа машинного кода программы, который ставит своей целью понять принцип работы, восстановить алгоритм, обнаружить недокументированные возможности программы и т. п.
Стилер	От англ. Stealer (вредоносная программа для кражи данных). Вредоносная программа, которая незаметно собирает большое количество конфиденциальной информации с зараженных устройств, например логины и пароли, данные платежных карт
Хакатоны	Соревнования или интенсивные командные мероприятия, в ходе которых участники за ограниченное время создают прототипы цифровых решений, продуктов или сервисов
Эксплойт	От англ. Exploit. Вредоносный код, который использует ошибки или недостатки системы безопасности для распространения киберугроз