УТВЕРЖДАЮ

Директор Национального координационного центра по компьютерным инцидентам

_____ О.В. Скрябин

«08» июля 2026 г.

Исходные данные для определения типа компьютерной атаки

Настоящие Исходные данные являются методическими рекомендациями, предназначенными для органов (организаций), осуществляющих в силу закона или на основании соглашения направление информации о компьютерных атаках в Национальный координационный центр по компьютерным инцидентам (НКЦКИ), и должны использоваться вместе с утвержденной в органе (организации) политикой информационной безопасности. Пороговые значения, содержащиеся в Исходных данных, приведены для примера из общей практики. При направлении в НКЦКИ информации орган (организация) предоставляют максимальное количество имеющихся материалов, содержащихся в пункте 5 соответствующего раздела Исходных данных. Отсутствие одного или нескольких материалов, подлежащих направлению в НКЦКИ, содержащихся в пункте 5 соответствующего раздела Исходных данных, не может являться основанием для непредставления остальных имеющихся материалов.

I. DDoS-атака.

1. Определение.

DDoS-атака (Distributed Denial of Service) – это компьютерная атака, направленная на перегрузку ресурсов целевой системы (сервера, сети, приложения) с целью нарушения её доступности для легитимных пользователей.

2. Ключевые признаки:

- аномально высокий трафик – резкий рост входящего сетевого трафика, особенно с множества IP-адресов;

- нестандартные запросы – массовые HTTP/HTTPS-запросы, UDP-флуд, SYN-флуд, ICMP-флуд и другие виды flood-атак;

- загрузка ресурсов системы – высокая загрузка CPU, памяти, сетевых интерфейсов;

- географическая распределённость источников – атака исходит из разных стран, AS, подсетей;

- нехарактерное количество обращений (в том числе легитимных).

3. Критерии классификации.

Событие информационной безопасности относится к домену «DDoS-атака», если наблюдаются одновременно:

- аномально высокий трафик (например, в 10 и более раз выше нормы);

- атака исходит из множества источников (ботнет, прокси, VPN).

4. Что НЕ является DDoS-атакой:

- одиночный DoS (не распределённый) – если атака идёт с одного IP;

- сканирование портов – это сетевая разведка, а не перегрузка ресурсов;

- высокая нагрузка из-за легитимного трафика.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) логи сетевого трафика:

- NetFlow/sFlow данные за период атаки;

- дампы трафика (PCAP) с примерами аномальных пакетов;

б) журналы защиты:

- логи межсетевого экрана (NGFW), IDS/IPS;

- данные от систем анти-DDoS (если применялись);

в) технические детали атаки:

- вектор атаки (HTTP-флуд, SYN-флуд, UDP-флуд и т. д.);
- основные и управляющие IP-адреса атакующих (если возможно выделить);
- порт(-ы) назначения и протоколы;

г) сведения о влиянии на инфраструктуру:

- графики нагрузки и статистические данные (CPU, RAM, сетевые интерфейсы).

- время начала и окончания атаки (UTC);

д) дополнительные данные:

- скриншоты панелей мониторинга (если есть аномалии).

- любые другие артефакты (например, подозрительные User-Agent'ы в HTTP-флуде).

II. Неудачные попытки авторизации.

1. Определение.

Неудачные попытки авторизации – это повторяющиеся попытки входа в систему с неверными учетными данными, которые могут указывать на подбор учетных данных (брутфорс), попытку использования утекших паролей, активность скомпрометированных учетных записей.

2. Ключевые признаки:

- множественные failed login в журналах аутентификации;

- попытки входа под разными учетными записями с одного IP;

- использование распространенных комбинаций логин/пароль;

- необычное время попыток входа (ночное, выходные);

- географически аномальные локации входа;

- запрос kerb-билета;

- обращение к серверу аутентификации: LDAP, Keycloak и т.д.

3. Критерии классификации.

Событие информационной безопасности относится к домену «неудачные попытки авторизации», если выполнено одно или несколько из следующих условий:

- наблюдается серия неудачных попыток входа (более 5-10 за короткий период);

- есть признаки автоматизированных попыток (высокая частота, шаблонность, в поле User-Agent есть название ПО);

- используются известные уязвимые комбинации.

4. Что НЕ является неудачными попытками авторизации:

- единичные ошибки ввода пароля пользователем, не более 4-х раз;

- проблемы с проверочным защитным текстом (CAPTCHA) или двухфакторной аутентификацией (2FA);

- ошибки «account locked» без предшествующих попыток входа;

- сбой в работе СПО, вызвавший срабатывание правила по признаку – одна и та же комбинация логин/пароль.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) журналы аутентификации:

- логи Active Directory, /var/log/auth.log, SSO-систем;

- временные метки каждой попытки авторизации;

б) данные об атакующем:

- IP-адреса (с whois-информацией);

- User-Agent строки;

- используемые учетные записи и название домена;

- используемые злоумышленником пароли;

в) контекст атаки:

- целевые системы/сервисы;

- используемые протоколы (RDP, SSH, WEB-форм);

- период активности;

г) дополнительные артефакты:

- примеры использованных паролей (если есть паттерн);

- скриншоты событий из SIEM;

- данные блокировок (если применялись);

- добавленные ключи (SSH);

- конфигурационные файлы служб входа (pam, sshd);

- JA3 – отпечаток, sni.

III. Попытки внедрения ВПО.

1. Определение.

Попытки внедрения вредоносного программного обеспечения (ВПО) – это действия злоумышленников, направленные на загрузку и выполнение вредоносного кода в целевой системе.

2. Ключевые признаки:

- подозрительные файлы (исполняемые файлы, скрипты, документы с макросами);

- несанкционированные изменения в реестре, автозагрузке, задачах планировщика;

- аномальная сетевая активность (C2-трафик, подключения к подозрительным доменам/IP);

- попытки эксплуатации уязвимостей для выполнения кода;

- использование уязвимых приложений (браузеры, офисные пакеты, ПО для удаленного доступа).

3. Критерии классификации.

Событие информационной безопасности относится к домену «попытки внедрения ВПО», если выполнено одно или несколько из следующих условий:

- обнаружены попытки загрузки/запуска подозрительных файлов;

- выявлены признаки эксплуатации уязвимостей для выполнения кода;

- найдены артефакты, указывающие на использование известных семейств ВПО;

- зафиксированы попытки сохранить вредоносный код в системе;

- события зафиксированы в журналах ABC, EDR.

4. Что НЕ является попытками внедрения ВПО:

- ложные срабатывания антивируса на легитимное ПО;

- подозрительные файлы, не подтвержденные в качестве вредоносных;

- сетевые атаки без попыток выполнения вредоносного кода.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) артефакты ВПО:

- подозрительные файлы (в изолированной среде);

- хэши (MD5, SHA-1, SHA-256);

- результаты анализа;

- атрибуты и хэш-суммы системных исполняемых модулей и загружаемых библиотек;

б) журналы событий:

- логи антивируса/EDR;

- журналы Windows (Event Log) или syslog;

- данные SIEM;

в) контекст атаки:

- вектор проникновения (фишинг, эксплуатация уязвимости и т.д.);

- временные метки событий;

- затронутые системы;

г) дополнительные данные:

- сетевые индикаторы (IP, домены, URL);

- скриншоты подозрительной активности;

- результаты динамического анализа (если проводился).

IV. Попытки эксплуатации уязвимости.

1. Определение.

Попытка эксплуатации уязвимости – это целенаправленные действия злоумышленника по использованию известной уязвимости или уязвимости «нулевого дня» в программном обеспечении, оборудовании или конфигурации системы для получения несанкционированного доступа, повышения привилегий пользователя или нарушения работы системы.

2. Ключевые признаки:

- нестандартные сетевые пакеты, соответствующие эксплойтам;

- попытки выполнения специфических команд через уязвимые интерфейсы;

- использование публичных эксплойтов (известные PoC-коды);

- аномальное поведение уязвимых сервисов (аварийные завершения, ошибки);

- попытки доступа к защищенным областям памяти (переполнение буфера).

3. Критерии классификации.

Событие информационной безопасности относится к домену «попытки эксплуатации уязвимости», если выполнено одно или несколько из следующих условий:

- обнаружены сетевые пакеты, соответствующие известным эксплойтам;

- зафиксированы попытки выполнения эксплойт-кода;

- выявлены аномалии в работе уязвимых сервисов;

- есть совпадение с сигнатурами известных уязвимостей;

- нарушена целостность исполняемых модулей и загружаемых библиотек .

4. Что НЕ является попытками эксплуатации уязвимости:

- сканирование на наличие уязвимостей без попыток эксплуатации;

- ложные срабатывания систем обнаружения;

- легитимное тестирование безопасности с разрешения.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) технические детали атаки:

- полные дампы сетевого трафика (pcap);

- точное название/идентификатор уязвимости (CVE ID);

- используемый вектор атаки;

б) журналы и артефакты:

- логи межсетевых экранов и IDS/IPS, узловых датчиков;

- дампы памяти атакованного сервиса;

- результаты анализа эксплойта;

- перечень системных вызовов, прерываний подозреваемого процесса;

в) контекст воздействия:

- временные метки атаки;

- целевые системы и сервисы;

- уровень доступа, полученный в результате атаки;

г) дополнительные данные:

- индикаторы компрометации (IoC);

- скриншоты аномальной активности;

- рекомендации по устранению уязвимости.

V. Публикация мошеннической информации.

1. Определение.

Публикация мошеннической информации – это размещение в информационных системах или сетях недостоверных, поддельных или вводящих в заблуждение данных с целью обмана пользователей, получения незаконной выгоды или нанесения ущерба репутации.

2. Ключевые признаки:

- поддельные веб-страницы, имитирующие легитимные ресурсы;

- фишинговые сообщения (email, мессенджеры, соцсети);

- фейковые объявления или предложения;

- модифицированный контент (измененные изображения, документы);

- социальные инженерные схемы (фальшивые аккаунты поддержки).

3. Критерии классификации.

Критерии классификации.

Событие информационной безопасности относится к домену «публикация мошеннической информации», если выполнено одно или несколько из следующих условий:

- обнаружены поддельные ресурсы, имитирующие легитимные;

- выявлены попытки сбора конфиденциальных данных через фальшивые формы;

- зафиксировано распространение заведомо ложной информации;

- установлен факт намеренного введения пользователей в заблуждение.

4. Что НЕ является публикацией мошеннической информации:

- непреднамеренные ошибки в публикуемой информации;

- спам-рассылки без элементов мошенничества;

- легитимные маркетинговые кампании.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) доказательства мошенничества:

- скриншоты поддельных страниц/сообщений и легитимных страниц/сообщений;

- полные заголовки фишинговых писем;

- URL фальшивых ресурсов и легитимных (при наличии);

б) технические данные:

- IP-адреса и домены мошенников;

- Whois-информация о доменах;

- логи доступа к поддельным ресурсам;

в) контекст атаки:

- целевая аудитория мошенников;

- используемые социальные инженерные методики;

- период активности;

г) дополнительные артефакты:

- информация о пострадавших (если имеется);

- данные о финансовых потерях (если применимо).

VI. Сетевое сканирование.

1. Определение.

Сетевое сканирование – это процесс активного исследования сетевой инфраструктуры с целью выявления доступных хостов и сервисов, открытых портов и протоколов, конфигурационных слабостей, архитектурных особенностей сети.

2. Ключевые признаки:

- массовые запросы к последовательности IP-адресов;

- систематические проверки портов (TCP/UDP);

- использование сканирующих утилит (Nmap, Masscan, Zmap);

- аномальные временные паттерны запросов;

- попытки определения ОС и сервисов (баннерный граббинг).

3. Критерии классификации.

Событие информационной безопасности относится к домену «сетевое сканирование», если выполнено одно или несколько из следующих условий:

- обнаружены систематические проверки диапазонов IP;

- зафиксированы попытки сканирования портов;

- выявлено использование известных сканирующих инструментов;

- наблюдается характерная последовательность запросов.

4. Что НЕ является сетевым сканированием:

- единичные ошибочные подключения;

- легитимные проверки доступности сервисов;

- автоматизированные тесты мониторинговых систем;

- фоновый интернет-шум (фоновое сканирование).

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) технические данные сканирования:

- дампы сетевого трафика (pcap);

- список целевых IP/портов;

- временные метки активности;

- используемые методы сканирования;

б) аналитические данные:

- результаты анализа инструментария;

- геолокация источников;

- частота осуществляемых запросов;

в) контекстные сведения:

- затронутые сегменты сети;

- потенциальные уязвимости, которые могли быть выявлены сканированием;

- связи с другими инцидентами;

г) дополнительные артефакты:

- сигнатуры IDS/IPS;

- логи межсетевых экранов;

- результаты обратного анализа источников;

- JA3 – отпечаток.

VII. Социальная инженерия.

1. Определение.

Социальная инженерия – это метод манипулирования людьми с целью получения конфиденциальной информации или доступа к защищенным системам, основанный на психологических приемах, а не на технических уязвимостях.

2. Ключевые признаки:

- незаконные запросы конфиденциальных данных (пароли, платежные реквизиты);

- поддельные уведомления (от службы безопасности, администрации);

- имитацию авторитетных лиц (руководство, IT-отдел, банки);

- физическое проникновение под ложным предлогом;

- использование факторов спешки/страха для давления на жертву.

3. Критерии классификации.

Событие информационной безопасности относится к домену «социальная инженерия», если выполнено одно или несколько из следующих условий:

- установлен факт психологического воздействия;

- выявлены попытки получения данных обходными путями;

- зафиксировано использование подложных документов/аккаунтов.

4. Что НЕ является социальной инженерией:

- технические атаки без человеческого фактора;

- автоматизированные брутфорс-атаки;

- ошибки сотрудников без фактора внешнего воздействия;

- попытки внедрения ВПО.

5. При передаче информации в НКЦКИ необходимо собрать и предоставить следующие материалы:

а) доказательства контакта:

- скриншоты переписки/сообщений;

- аудио/видео записи разговоров;
- копии поддельных документов;

б) технические данные:

- метаданные сообщений;
- почтовые заголовки;
- URL фишинговых страниц;

в) контекст атаки:

- описание схемы воздействия;
- целевые данные/системы;
- количество пострадавших;

г) дополнительные артефакты:

- идентификаторы мошенников;
- примеры используемых легенд;
- рекомендации по защите персонала.