УДК 004.056

МЕТОДИКА ФОРМИРОВАНИЯ СЦЕНАРИЕВ РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ НА ОСНОВЕ БАЗ ЗНАНИЙ MITRE

Т. В. БОРБОТЬКО,
директор государственного предприятия «НИИ ТЗИ»

В основу предлагаемой методики положен жизненный цикл реагирования на киберинцидент NIST 800-61, а для определения целей, задач и соответствующих им мероприятий по противодействию нарушителю предлагается использовать информацию из баз знаний MITRE: ATT&CK, Engage и D3FEND.

ВВЕДЕНИЕ

В рамках реализации Указа Президента Республики Беларусь № 40 [1] в стране создаются центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры (далее – центры кибербезопасности (ЦКБ)) для противодействия внутренним и внешним угрозам по отношению к таким объектам. Требования, которым должны соответствовать ЦКБ, изложены в соответствующем приказе Оперативно-аналитического центра при Президенте Республики Беларусь [2], а реагирование на киберинциденты в том числе может быть реализовано с использованием положений стандарта NIST 800-61 [3].

Важные аспекты обеспечения реагирования на киберинциденты – наличие и содержание соответствующих сценариев. Они позволяют специалистам по информационной безопасности систематизировать процесс реагирования и минимизировать ошибки при принятии решения. Для составления сценария необходимо иметь описание угрозы информационной безопасности, определить цель и задачи на каждом из этапов реагирования на киберинцидент, а также выбрать и обосновать необходимые и достаточные мероприятия для противодействия нарушителю. В качестве источников информации, позволяющих получить необходимые сведения, предлагается использовать базу знаний MITRE. Процесс же составления сценария регламентируется предлагаемой методикой.

БАЗЫ ЗНАНИЙ MITRE

База знаний MITRE ATT&CK [4] чаще всего применяется специалистами по информационной безопасности и содержит в себе сведения о тактиках (Tactic), техниках (Technique), а также примеры программных средств (Procedure) (TTP), которые позволяют нарушителю реализовать соответствующие техники. На основании наименования техники в ней можно найти мероприятия, реализация которых позволяет обнаружить нарушителя (Detection) и обеспечить минимизацию ущерба (Mitigations) от его деятельности. Вместе с тем таких мероприятий для одной техники в базе знаний MITRE ATT&CK приводится множество, что существенно усложняет их выбор. Кроме этого, необходимо отметить, что процесс реагирования на киберинцидент, согласно NIST 800 61, представляет собой последовательность действий, направленных на локализацию нарушителя и противодействие ему, обеспечение сохранности активов информационной системы и восстановление бизнес-процессов организации после воздействия нарушителя на информационную систему.

Таким образом, рассматривать мероприятия по противодействию нарушителю необходимо как взаимосвязанные, адекватные применяемым им техникам и обеспечивающие достижение целей реагирования на киберинцидент.

База знаний MITRE Engage [5] содержит в себе информацию, которую можно использовать для формулирования целей и соответствующих

им задач противодействия нарушителю. Формулирование целей реализуется исходя из цикла деятельности специалиста по информационной безопасности, состоящего из трех этапов: подготовка (prepare), противодействие (operate), оценка (understand). Такой цикл, по своей сути, имеет аналогию с циклом Шухарта – Деминга [6].

Этап «противодействие» (operate) [5] в свою очередь делится на три подэтапа: обнаружение нарушителя (expose), противодействие ему (affect) и изучение его TTP (elicit). Каждый из подэтапов, декомпозируется в соответствующие подходы (approaches), которые реализуются за счет ряда мероприятий (activities), что позволяет уточнить цель противодействия нарушителю и сформулировать задачи, решение которых позволит ее достичь.

Например, подэтап «обнаружение нарушителя» (expose) реализуется за счет двух подходов: сбор информации (collect) и обнаружение нарушителя (detect). В свою очередь каждый из указанных подходов может быть реализован четырьмя мероприятиями. Реализация подхода «обнаружение нарушителя» (detect) обеспечивается с помощью мероприятий: заблаговременное внедрение уязвимостей и контроль их эксплуатации (introduced vulnerability), применение систем-ловушек (lures), динамический анализ наличия вредоносного кода в файлах (malware detonation), анализ сетевого трафика (network analysis). Для упрощения определения мероприятий графический интерфейс базы знаний позволяет их выбрать, например, по известной технике нарушителя, что обеспечивает взаимосвязь между сведениями, представленными как в базе знаний MITRE ATT&CK, так и MITRE Engage.

Необходимо отметить, что на формулировки целей и связанных с ними задач применяемые нарушителем техники оказывают влияние только на этапе противодействия (operate). Исходя из этого, цели и задачи, определяемые в различных сценариях реагирования на киберинцидент на этапах «подготовка» (prepare) и «оценка» (understand), будут схожими, а их отличие будет состоять в применяемых тактиках противодействия нарушителю.

База знаний MITRE D3FEND [7] содержит информацию о тактиках и техниках противодействия нарушителю, которые структурированы в рамках цикла, имеющего сходство с циклом реагирования на киберинцидент NIST 800-61. Этапы противодействия нарушителю, представленные в MITRE D3FEND, следующие: анализ угроз и защищаемой информационной системы (model), защита информационной системы (harden), обнаружение нарушителя в информационной системе (detect), сегментирование информационной системы (isolate), применение систем-ловушек (decive), удаление нарушителя из информационной системы (evict) и восстановление информационной системы после воздействия нарушителя (restore). Каждый из этапов может быть реализован с помощью соответствующих тактик, которые, в свою очередь, представлены определенными техниками.

Например, этап «обнаружение нарушителя в информационной системе» (detect) реализуется такими тактиками, как анализ файлов (File Analysis), анализ идентификаторов (Identifier Analysis), анализ сообщений (Message Analysis), анализ сетевого трафика (Network Traffic Analysis), мониторинг аппаратно-программных средств (Platform Monitoring), мониторинг процессов (Process Monitoring), анализ действий пользователя (User Behavior Analysis). В свою очередь тактика «анализ сообщений» (Message Analysis) реализуется с помощью таких техник, как анализ рейтинга доверия к программному обеспечению отправителя сообщения (Sender MTA Reputation Analysis) и анализ рейтинга доверия к отправителю сообщения (Sender Reputation Analysis).

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Деятельность специалиста по информационной безопасности целесообразно рассматривать через призму процессного подхода [6]. Он основывается на формулировании цели, а, по сути, тех результатов, которых необходимо достичь. Цели, в свою очередь, декомпозируются в соответствующие им задачи. Кроме этого, процессный подход предполагает анализ исходных сведений, позволяющих определить взаимосвязанные мероприятия для достижения поставленной цели, и выделение требуемых ресурсов для реализации мероприятий. Учитывая вышеизложенное, предлагается следующая методика формирования сценариев реагирования на киберинцидент.

На первом этапе (рисунок 1) обеспечивается формулирование целей и определение соответствующих им задач. Для его реализации предлагается использовать информацию, представленную в базе знаний MITRE Engage. Исходными сведениями для реализации замысла этапа является наличие информации о техниках, которые использует нарушитель при проведении кибератаки. Учитывая это, рассмотрим пример формулирования целей и задач на этапе противодействия (operate), а в качестве техники возьмем из базы знаний MITRE ATT&CK одну из наиболее распространенных – эксплуатация уязвимостей в общедоступном приложении (T1190) [8].

Пользуясь описанием подэтапа «обнаружение нарушителя» (expose) из базы знаний MITRE Engage, сформулируем цель противодействия: обнаружение нарушителя, получившего или получающего доступ к информационной сети организации. Для определения адекватных технике мероприятий и формулирования задач, решение которых позволит достичь цели, используя

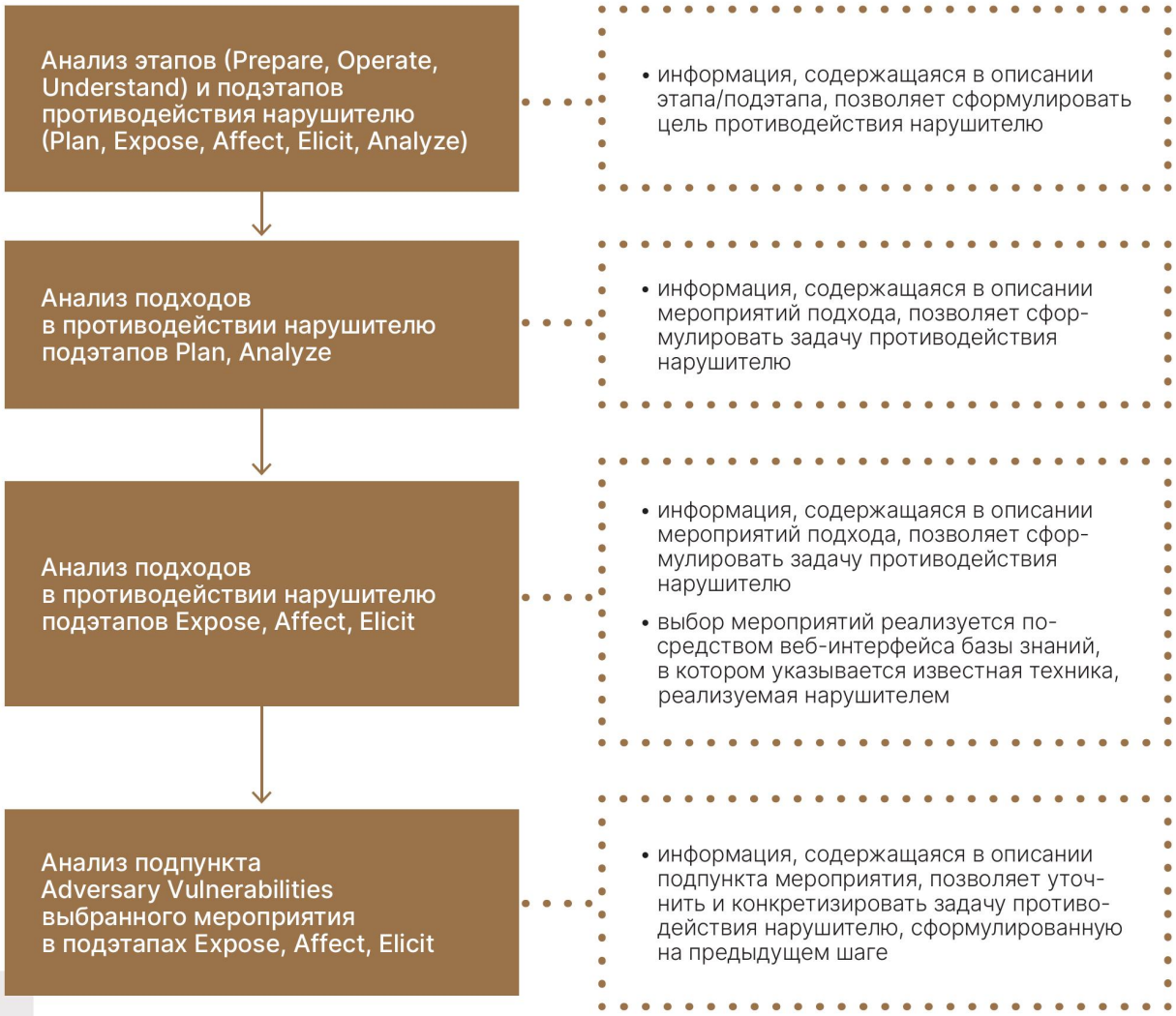

Рисунок 1. Последовательность действий первого этапа методики

графический интерфейс базы знаний, выполним выбор мероприятий, учитывая вышеуказанную технику. Необходимо отметить, что выбор мероприятий, используя графический интерфейс базы знаний MITRE Engage, можно реализовать не по одной, а нескольким техникам.

Исходя из полученного результата, для обнаружения нарушителя необходимо использовать приманки (lures), в качестве которых выступает такое программно-технические средство, как honeypot [9]. Техника T1190 предполагает эксплуатацию уязвимости в общедоступном приложении, которую может обнаружить нарушитель, до того момента, пока она будет устранена специалистом по информационной безопасности. Поэтому для снижения риска компрометации информационной системы нарушителем в нее заблаговременно вводится общедоступное приложение, которое имеет уязвимость, а ее эксплуатация контролируется системой мониторинга. Такое приложение в защищаемой информационной системе играет роль приманки для нарушителя, и его взаимодействие с ним должно позволить достичь определенной цели.

Исходя из вышеизложенного, сформулировать задачу, соответствующую такой цели, можно следующим образом: выбрать и обосновать программно-технические средства типа honeypot. Для обоснования их характеристик, кроме анализа особенностей реализации техники T1190, которые можно уточнить, анализируя информацию, представленную в базе знаний MITRE ATT&CK, необходимо обратить внимание на сведения, изложенные в базе знаний MITRE Engage в подпункте «уязвимости нарушителя» (adversary vulnerabilities), входящем в описание мероприятия приманки (lures) подэтапа «обнаружение нарушителя» (expose). Анализ этой информации позволит уточнить и конкретизировать задачу. Аналогичным образом формулируются цели и задачи подэтапов противодействия нарушителю (affect) и изучение его TTP (elicit).

Рисунок 2. Последовательность действий второго этапа методики

Исходя из сформулированных целей и задач, на **втором этапе** методики определяются мероприятия, практическая реализация которых позволит достичь поставленных целей (рисунок 2). С учетом того, что реагирование на киберинцидент реализуется в соответствии с требованиями NIST 800-61, для определения мероприятий предлагается использовать информацию, содержащуюся в базе знаний MITRE D3FEND. Графический интерфейс базы знаний позволяет вести поиск необходимых сведений исходя из, например, известной техники, которую может реализовать нарушитель. На рисунке 3 демонстрируются способы, имеющиеся в базе знаний MITRE D3FEND (этап «обнаружение» (detect)), позволяющие обеспечить противодействие нарушителю в случае реализации им техники T1190.

Обнаружение реализуемой нарушителем техники T1190 (рисунок 3) может быть выполнено за счет анализа: исходящего сетевого трафика

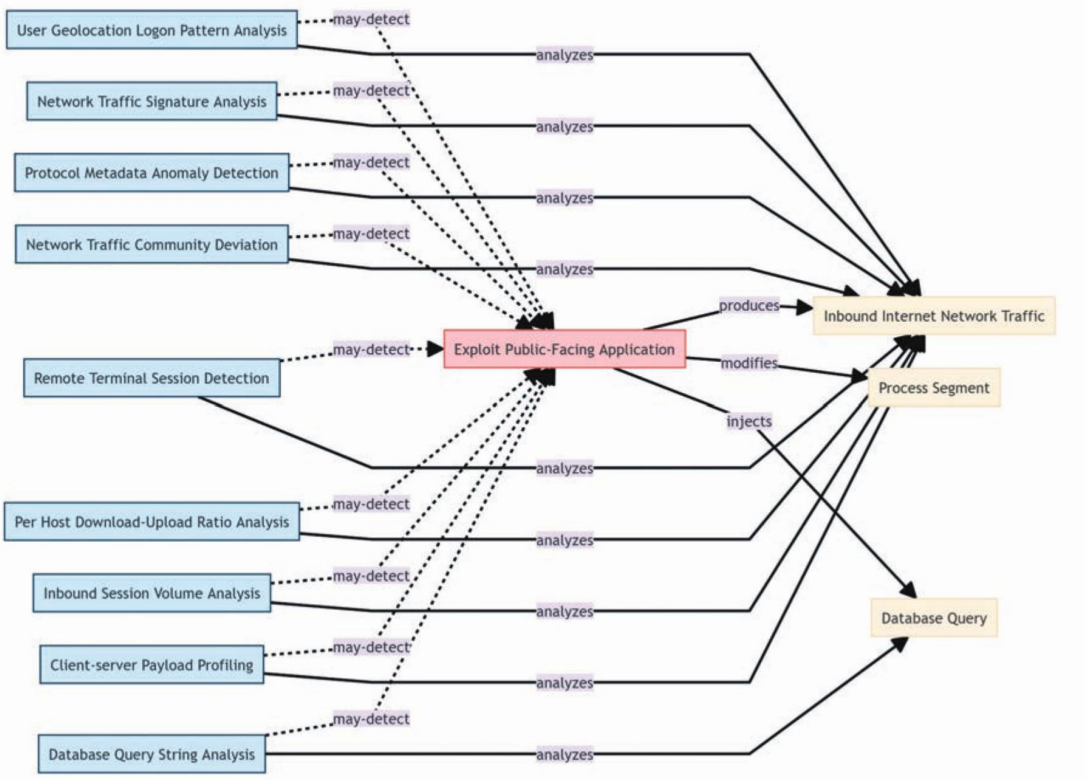

Рисунок 3. Способы, позволяющие обнаружить нарушителя, который применяет технику T1190

(Inbound Internet Network Traffic) или запросов к базе данных (Database Query). Затем выбираются доступные для данной информационной системы мероприятия и реализующие их средства, в данном случае средства мониторинга. Например, в случае принятия решения об анализе запросов к базе данных можно использовать только одно мероприятие (рисунок 3): анализ параметров строки запроса к базе данных (Database Query String Analysis), которое позволяет обеспечить обнаружение SQL-инъекции. В случае если реализация техники T1190 нарушителем приводит к формированию исходящего сетевого трафика, то спектр мероприятий насчитывает восемь позиций, среди которых специалист выбирает наиболее подходящие для достижения цели. Выбор мероприятий позволяет обосновать применение программно-технических средств, которые обеспечат их реализацию.

Выбор соответствующих мероприятий по противодействию нарушителю реализуется на каждом из этапов жизненного цикла реагирования на киберинцидент [3].

ЗАКЛЮЧЕНИЕ

Предложенная методика позволяет систематизировать деятельность специалиста по информационной безопасности при формировании им сценария реагирования на киберинцидент, который состоит из ряда этапов, согласно NIST 800-61. На каждом из этапов формулируются цель и задачи, для описания которых используются сведения, имеющиеся в базе знаний MITRE Engage, а соответствующие им мероприятия формируются на основе сведений из базы знаний MITRE D3FEND. Для каждого сценария важным аспектом является понимание и описание угрозы информационной безопасности (этап подготовки, в соответствии с NIST 800-61), исходя из сущности которой определяется порядок реагирования на нее. Исходные данные, позволяющие осмыслить сущность угрозы, представлены описанием техник, которые реализует нарушитель при проведении кибератаки. Подобные сведения имеются в базе знаний MITRE ATT&CK, а последствия, которые могут наступить вследствие реализации нарушителем определенной техники, можно найти в базе знаний MITRE D3FEND. Понимание сущности угрозы является важным для целенаправленной деятельности специалиста по информационной безопасности. Осознание им последствий кибератаки позволяет ему обосновать необходимые для противодействия ресурсы перед руководством организации.

Предложенная методика может быть использована при формировании и актуализации сценариев реагирования на киберинцидент в ЦКБ, а также в подразделениях организаций, обеспечивающих их кибербезопасность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Указы Президента Республики Беларусь // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: https://www.oac.gov.by/public/content/files/files/law/decrees-rb/2023-40.pdf (дата обращения: 24.02.2025).
2. Указы Президента Республики Беларусь // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf (дата обращения: 24.02.2025).
3. Computer Security Resource Center // National Institute of Standards and Technology. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (date of access: 24.02.2025).
4. ATT&CK Matrix for Enterprise // MITRE ATT&CK. – URL: https://www.attack.mitre.org (date of access: 24.02.2025).
5. MITRE Engage Framework // MITRE Engage. – URL: https://www.engage.mitre.org (date of access: 24.02.2025).
6. Аудит информационной безопасности / А.П. Курило [и др.]. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
7. MITRE D3FEND Matrix // MITRE D3FEND. – URL: https://www.d3fend.mitre.org (date of access: 24.02.2025).
8. Итоги проектов по расследованию инцидентов и ретроспективному анализу – 2023-2024 // Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/itogi-proektov-po-rassledovaniyu-inczidentov-i-retrospektivnomu-analizu-2023-2024 (дата обращения: 24.02.2025).
9. 70+ бесплатных приманок для ловли хакеров // Habr. – URL: https://habr.com/ru/companies/bastion/articles/731172/ (дата обращения: 24.02.2025).

The proposed methodology is based on the NIST 800-61 cyber incident response life cycle, and to determine the goals, objectives and corresponding measures to counter the intruder, it is proposed to use information from the MITRE knowledge bases: ATT&CK, Engage and D3FEND.

Статья поступила в редакцию 05.06.2025.