DEVELOPMENT OF AN AGROCALCULATOR FOR CALCULATING FERTILIZERS USING THE JAVASCRIPT PROGRAMMING LANGUAGE

T.Zh. Bazarzhapova, T.N. Maltseva

The article discusses the development of a calculator for calculating fertilizers. The general view and method of calculation of fertilizers are presented. The technology of developing a calculator using the JavaScript programming language is described. Such use of digital technologies in agriculture will help to reduce costs and increase crop yields.

Key words: agrocalculator, programming, JavaScript, MySQL database, PHP, fertilizer dosage, website.

Bazarzhapova Tuya Zhamyanovna, candidate of pedagogical sciences, docent, btuyazh@gmail.com, Russia,Ulan-Ude, Buryat State Agricultural Academy named after V.R. Filippov,

Maltseva Tatyana Nikolaevna, master, Russia,Ulan-Ude, Buryat State Agricultural Academy named after V.R. Filippov

УДК 004.056.5
DOI: 10.24412/2071-6168-2022-8-116-121

МЕТОДИКА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

С.А. Веревкин, А.В. Кравчук, М.И. Беляков

В статье рассмотрена актуальная проблема, связанная с решением задачи оперативного реагирования на инциденты информационной безопасности на объектах критической информационной инфраструктуры. На основе открытых источников данных о популярных уязвимостях, техниках, тактиках и процедурах, используемых злоумышленниками при реализации атакующих воздействий, предложен проект методики решения поставленной задачи. Предложенная методика содержит несколько этапов, включающих комплексный анализ структуры объекта информатизации, определение актуальных тенденций проведения атакующих воздействий, их классификацию и определение методов противодействия или компенсации ущерба от реализованных атакующих воздействий. Также, методика подразумевает выработку инструкций для наиболее популярных и актуальных для информационной системы сценариев атак. Таким образом, формируется набор типовых шаблонов противодействия, что способствует оперативному принятия решений в случае возникновения подобных инцидентов.

Ключевые слова. информационная безопасность, управление инцидентами, критическая информационная инфраструктура, защита информации, реагирование на инциденты.

В современном динамично развивающемся мире, нельзя не выделить роль процесса защиты информации. Важность данного процесса заключается в значительном росте стоимости информации, а также возможности получения конкурентных преимуществ на рынке. В рамках данной работы, предложена методика анализа защищенности и управления инцидентами в автоматизированных системах, отнесенных объектам критической информационной инфраструктуры (КИИ) [1].

Условие отнесения объекта защиты информации к КИИ, требует поддержания состояния защищенности информационных систем объекта в актуальном состоянии. Причиной необходимости регулярной актуализации системы защиты является то, что несвоевременное реагирование на инциденты может привести не только к нарушению основных аспектов информационной безопасности, но и к невозможности функционирования объекта защиты в целом [ФЗ о безопасности критической информационной инфраструктуры].

В рамках действующих требований законодательства, задачи прогнозирования инцидентов, контроля защищенности, расследования инцидентов и обеспечения взаимодействия между организациями, реализуются посредством подключения организации к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

Однако, несмотря на централизованный характер системы ГосСОПКА, стоит отметить существенные временные затраты на межведомственную коммуникацию и реагирования при возникновении инцидентов.

Таким образом, существует необходимость внедрения внутренней частной методики анализа состояния защищённости и управления инцидентами объекта КИИ, реализация которой является задачей SOC (Security Operation Center) организации.

Постановка задачи. Основной целью разрабатываемой методики является определение действий сотрудников SOC организации в случае необходимости оперативного реагирования на инциденты информационной безопасности, в частности на компьютерные атаки на сетевую инфраструктуру организации, а также при проведении расследований.

Исходя из цели разрабатываемой методики, необходимо выделить основные задачи:

- оценивание состояния исследуемой системы в реальном времени – суть задачи состоит в постоянном мониторинге сетевой инфраструктуры и сервисов объекта защиты. Также, в рамках данной задачи требуется проведение мониторинга сетевого трафика для дальнейшего анализа;
- выработка показателей исследуемой сети – основываясь на анализе данных, полученных на первом этапе методики, формируется модель исследуемой сети организации, содержащая сведения об устройствах сети, используемом программном обеспечении, протоколах и др. данные, необходимые для комплексного анализа сети;
- формирования перечня воздействий, характеризующих инциденты информационной безопасности – задача подразумевает определение перечня уязвимостей, характерных для программного обеспечения, протоколов и устройств сети. Также, необходимо дополнение перечня уязвимостей, набором техник, тактик и процедур (TTP) в соответствии с актуальной версией методики оценки угроз безопасности информации ФСТЭК [2].
- выявление атакующих воздействий и требований к реагированию – вырабатывается дополнительный перечень метрик для систем защиты информации, на основе которых происходит классификация инцидентов. Также, в соответствии с реализованной в организации концепцией управления рисками информационной безопасности, вырабатывается унифицированный подход к реагированию на инцидент.

На основе задач разрабатываемой методики, определим её основные этапы для объектов критической информационной инфраструктуры:

1) **Мониторинг сетевой инфраструктуры объекта КИИ.** Первоначальной задачей является сбор данных о текущем состоянии объекта КИИ и формирования перечня, используемых в его составе аппаратных и программных решений.

Итогом этапа является структурированный перечень используемых в составе информационной системе объекта КИИ программных, аппаратных и иных решений.

2) **Анализ событий в сети КИИ.** На основе анализа собранных ранее данных, формируется модель информационной инфраструктуры объекта защиты. На основе полученных дампов сетевого трафика, а также открытых данных баз данных Mitre (ATT&CK[3], CVE[4], CPE[5], CWE[6], CAPEC[7]) и БДУ ФСТЭК[8], разрабатывается набор метрик, характеризующих нормальную и аномальную активность внутри сети объекта КИИ.

1. Формирование шаблонов нормального поведения в сети организации реализуется на основе результатов, полученных при сканировании сети. Также, следует отметить необходимость анализа дампов сети на предмет выявления вредоносной активности, для исключения возможности отнесения подобных сигнатур к нормальной сетевой активности. Зачастую, профиль нормального поведения в сети объекта защиты, формируется системами защиты информации объекта КИИ, например, при внедрении DLP (систем предотвращения утечки информации).

2. Разработка показателей аномальной активности в сети объекта КИИ реализуется в результате формирования комплексного перечня уязвимостей баз Mitre и ФСТЭК. Исходный перечень уязвимостей должен содержать следующие данные:

описание уязвимости;

результаты оценки уязвимости в соответствии с выбранной методикой оценки угроз, например, CVSS v.3, CVSS v.2 и др.

техники, тактики и процедуры (TTP) при реализации которых, реализуется эксплуатация уязвимости, характеризующие вектор проведения сложных атак;

наличие конкретных эксплойтов для реализации уязвимости;

версии программного обеспечения, в которых возможна реализация уязвимости;

рекомендуемые меры и средства устранения уязвимости.

Таблица 1

Перечень потенциальных источников данных и инструментов для получения хранящейся в них информации

№	Источник данных	Данные	Инструментарий
1	сеть организации	дампы сети, содержащие сведения об используемой в сети адрессации, используемых протоколах, сервисах и службах, сетевых устройствах, прикладном и системном программном обеспечении	Снифферы, например Wireshark, TCPdump, CommView и др.
2	система защиты информации и журналы событий узлов сети	журналы операционных систем, сетевых устройств и систем защиты информации, содержащие сведения о действиях пользователей и инцидентах, характерных для конкретной сети объекта КИИ.	Для ОС Windows: C:\Windows\System32\winevt\Logs\ Для ОС Linux: /var/log Прочие: система журналирования сетевых устройств и систем защиты информации
3	операционная система	снятие образов оперативной памяти, жесткого диска	Belkasoft RAM Capturer Dumpit Linux Memory Extractor Rekall и др.
4	телекоммуникационное оборудование организации	настройки телекоммуникационного оборудования	Файлы конфигурации сетевого оборудования
5	интерфейсы устройств сети, реестры отдела делопроизводства	перечень аппаратных компонентов устройств в сети	Aida64 Реестры, содержащие сведения об аппаратных компонентах сети и др.
6	интерфейсы устройств сети, дампы сети	перечень установленного программного обеспечения и версий прошивок сетевого оборудования	Aida64 Wireshark Интерфейс системы и др.
7	служба Active Directory	набор используемых политик организации	SRAT ADUC и др.
8	прочие источники данных	иные сведения	-

Затем, формируется перечень актуальных уязвимостей объекта КИИ. Актуальность уязвимостей определяется посредством сопоставления данных об объекте защиты, общему перечню уязвимостей. В результате сопоставления, создается перечень уязвимостей характерных для информационной инфраструктуры объекта защиты. Дополнительно, перечень актуальных уязвимостей может дополняться популярными уязвимостями и связанные с потенциально исполнимыми техниками и тактиками уязвимости перечень которых составляется на основе современных тенденций реализации атак.

3) **Классификация инцидентов, характерных для объекта КИИ.** Создается классификация уязвимостей информационной безопасности, сопоставленный перечню техник, тактик и процедур, характеризующих этапы реализации атак злоумышленником.

Итоговая классификация формируется в виде таблицы, содержащей следующие данные:

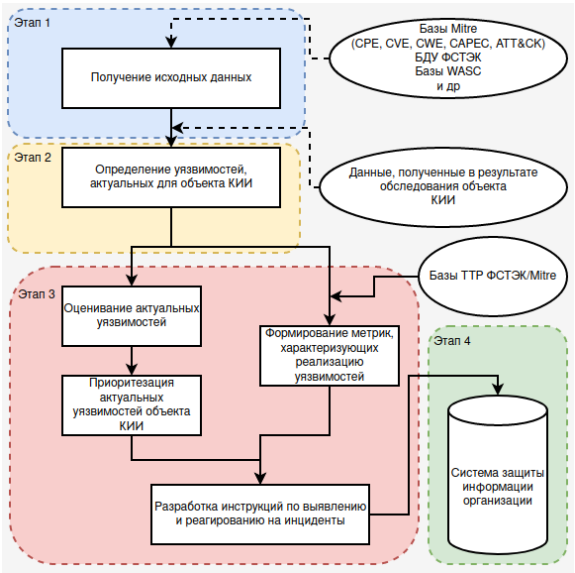
- класс инцидента;
- суть инцидента;
- результаты оценки уязвимости;
- показатели, характеризующие эксплуатацию уязвимости;
- методы компенсации / противодействия использованию уязвимости;
- сроки устранения уязвимости.

Данные таблицы являются комплексным представлением информации об инциденте, что в свою очередь, дает возможность специалистам SOC оперативно реагировать на инциденты. Одним из наиболее важных показателей, является «срок устранения уязвимости», определяемый специалистами по защите информации объекта КИИ, в соответствии с классами инцидента.

Стоит отметить, что таблица, также должна содержать метрики, в соответствии с которыми было принято решение о существовании конкретного инцидента. Подобное представление позволяет существенно снизить аналитическую работу специалиста по безопасности и способствует принятию решения об актуальности инцидента, в случае ложных срабатываний систем защиты.

4) **Интеграция полученных данных в систему защиты информации объекта КИИ.** Заключительным этапом методики является адаптация полученных данных для использования в действующей системе защиты. Полученные данные об инцидентах, в том числе метрики, сформированные на основе поведенческого анализа, переносятся оператором центра безопасности объекта КИИ в систему защиты информации.

Наиболее ярким примером является разработка правил для системы обнаружения вторжений на основе полученных показателей аномального воздействия. Подобное решение позволит не только выявлять аномальное поведение в сети организации на ранних этапах реализации атаки, но и осуществлять блокировку подозрительных пакетов, позволяя тем самым идентифицировать текущие возможности нарушителя и получить временной промежуток на принятие решения о дальнейшем противодействии. Обобщенная схема этапов разрабатываемой методики представлена на рисунке.



Обобщенная схема этапов разрабатываемой методики

Заключение. В ходе работы была предложена реализация методика анализа текущей защищенности и управления инцидентами информационной безопасности объектов критической информационной инфраструктуры. Разработанная методика содержит комплексный подход к анализу большого объема данных инцидентов безопасности, включая поведенческий анализ действий злоумышленника на основе популярных зарубежных и отечественных методик.

Также, в методике предложена концепция структуры представления данных об инцидентах, позволяющая специалисту SOC оперативно реагировать при возникновении инцидентов, а также в случае ложных срабатываний систем защиты информации. Отметим сложность разработки унифицированных показателей атакующих воздействий, по причине необходимости обработки большого объема данных о реализации уязвимостей, однако, подобный подход может позволить повысить эффективность систем защиты информации, особенно, при использовании эвристических подходов к формированию метрик аномального поведения в сети.

Важно помнить, что без поддержания в актуальном состоянии баз знаний, на основе которых строится разрабатываемая методика, невозможно обеспечить комплексную защиту инфраструктуры объектов КИИ, по этой причине требуется их регулярная актуализация.

Список литературы

1. Указ Президента Российской Федерации от 30.03.2022 г. № 166. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации. М., 2022.

2. Методический документ ФСТЭК РФ «Методика оценки угроз безопасности информации» от 05.02.2021.

3. База техник, тактик и процедур, используемых злоумышленниками ATT&CK [Электронный ресурс] URL: https://attack.mitre.org (дата обращения: 10.05.2022).

4. База общих уязвимостей и рисков CVE [Электронный ресурс] URL: https://cve.mitre.org (дата обращения: 10.05.2022).

5. База общих платформ CPE (операционных систем и программного обеспечения) [Электронный ресурс] URL: https://cpe.mitre.org (дата обращения: 10.05.2022).

6. Общее перечисление слабых мест CWE [Электронный ресурс] URL: https://cwe.mitre.org (дата обращения: 10.05.2022).

7. Общие перечисления и классификации шаблонов атак CAPEC [Электронный ресурс] URL: https://capec.mitre.org (дата обращения: 10.05.2022).

8. Банк данных угроз безопасности информации БДУ ФСТЭК [Электронный ресурс] URL: https://bdu.fstec.ru/threat (дата обращения: 10.05.2022).

Веревкин Сергей Александрович, младший научный сотрудник научной лаборатории, vka@mil.ru, Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского, аспирант Санкт-петербургского федерального исследовательского центра российской академии наук,

Кравчук Алексей Владимирович, канд. техн. наук, начальник научной лаборатории, Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского,

Беляков Максим Игоревич, канд. техн. наук, начальник научной лаборатории, Россия, Санкт-Петербург, Военно-космическая академия им. А.Ф. Можайского

METHODOLOGY FOR MANAGING INFORMATION SECURITY INCIDENTS AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

S.A. Verevkin, A.V. Kravchuk, M.I. Belyakov

The article considers an urgent problem related to solving the problem of rapid response to information security incidents at critical information infrastructure facilities. Based on open data sources on popular vulnerabilities, techniques, tactics and procedures used by attackers in the implementation of attacking actions, a draft methodology for solving the task is proposed. The proposed methodology contains several stages, including a comprehensive analysis of the structure of the informatization object, determination of current trends in the conduct of attacking influences, their classification and determination of methods of countering or compensating for damage from implemented attacking influences. Also, the methodology implies the development of instructions for the most popular and relevant attack scenarios for the information system. Thus, a set of typical counteraction patterns is formed, which contributes to prompt decision-making in the event of such incidents.

Key words: information security, incident management, critical information infrastructure, information security, incident response.

Verevkin Sergey Aleksandrovich, junior researcher at the scientific laboratory, vka@mil.ru, Russia, Saint Petersburg, A.F. Mozhaisky Military Space Academy,

Kravchuk Alexey Vladimirovich, candidate of technical sciences, head of the scientific laboratory, Russia, Saint Petersburg, Military Space Academy named after A.F. Mozhaisky,

Belyakov Maxim Igorevich, candidate of technical sciences, head of the scientific laboratory, Russia, Saint Petersburg, Military Space Academy named after A.F. Mozhaisky