Описание инцидента при тестировании информационной безопасности киберфизических систем

В.Д. Михайлова

Южный федеральный университет, Таганрог

Аннотация: Цель исследования – провести анализ методик описания компьютерного инцидента в области информационной безопасности при выявлении неправомерных событий и тестировании киберфизических систем для повышения качества работы с документации при защите киберфизических систем. Для достижения цели необходимо выработать формат описания инцидентов. Для этого были проанализированы нормативно-правовые документы, выделены типы компьютерных инцидентов и их классификация, определены критерии инцидента и выявлены степени критичности последствий при их возникновении. Был выработан документ для описания инцидента. Данные исследования проводятся совместно с работами по выработке методик мониторинга и тестирования безопасности киберфизических систем для автоматического обнаружения неправомерной работы и(или) аномальной работы в киберфизической системе. По результатам исследований будет сформирован алгоритм действий и способы выявления и предотвращения последствий компьютерных инцидентов из-за чего можно будет повысить степень безопасности киберфизических систем.

Ключевые слова: событие информационной безопасности, компьютерный инцидент, информационная система, описание инцидента, формирование документации, карточка инцидента, кибербезопасность, киберфизическая система.

Введение

Киберфизическая система (КФС) – это система включающая в себя интернет вещей, автоматизированные системы управления, которые содержат в себе различные программные обеспечения и искусственный интеллект (ИИ) [1]. С развитием технологий стало необходимо оценивать, насколько безопасно они работают, не нарушая триаду конфиденциальности, целостности и доступности данных (КЦД). [2 - 4].

Задача, которую необходимо выполнить в рамках работы: проанализировать методы описания компьютерного инцидента в области информационной безопасности (ИБ) при выявлении неправомерных событий и тестирования КФС. В статье [5] описаны признаки инцидента, в результате чего можно предупреждать об инциденте ИБ в автоматизированных информационных системах (ИС), но данные признаки не описывают сам инцидент, его степень влияния и критичность в КФС. В статье [6] описан сравнительный анализ подходов реагирования на инциденты в разных

странах, но не описаны параметры, которые указывают при выявлении инцидента и дальнейшей работы с ним. В статье [7] на основе графовых моделей автор построил процесс ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Автор выдал каждой вершине вес (приоритет) и описал в каком порядке необходимо начинать работу при реагировании инцидентов. На основе проанализированной литературы можно сделать вывод, что ученные задаются вопросами выявления инцидентов и важности реагирования на инциденты. Но авторы не описывают инциденты и не описывают степень влияния их на работу КФС.

Классификация компьютерных инцидентов

Компьютерный инцидент – это вид инцидента ИБ, который несет в себе нарушение работы или изменения работы, обработки и приостановки функционала информационного ресурса (ГОСТ Р 59712-2022 "Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты"). Киберинцидент – это нарушение или неизбежная угроза нарушения политик ИБ, политик допустимого использования или стандартных практик ИБ (NIST SP 800-61 "Computer Security Incident Handling Guide"). Киберустойчивость — это способность ИС сохранять нормальное функционирование в условиях кибератак и противодействовать им в цифровой среде (ГОСТ Р 53114-2008 “Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения”).

На основе анализа литературы можно выявить новую классификацию компьютерных инцидентов на КФС по различным критериям:

1. Уровень серьезности: Блокирующий (Blocker) — из-за инцидента КФС совсем не работает, Критический (Critical) — когда инцидент влияет на главный функционал КФС, Серьезный (Major) — когда инцидент создает неудобства, но не влияет на КФС, Незначительный (Minor) — инцидент, который не влияет на “логику” работы КФС, Тривиальный (Trivial) —

инциденты этого уровня не влияют на работу и качество КФС. Такие инциденты не исправляют специально, а обычно исправляют в ходе столкновения с функционалом, который находится рядом.

2. Частота возникновения инцидента: В первый раз, Повторное возникновение.

3. Типы угроз: Угроза утечки конфиденциальной информации, Угроза несанкционированного доступа к данным или системам, Угроза неправомерной модификации, подделки или искажения данных, Угроза блокирования доступа (отказ в обслуживании), Угроза нарушения работоспособности систем или процессов, Угроза незаконного массового сбора конфиденциальной информации с целью ее неправомерного использования.

4. Преднамеренность возникновения: Преднамеренно, Непреднамеренно.

5. Нарушение свойств ИБ: КЦД.

6. Уровень информационной инфраструктуры: 1В — применяется при работе с конфиденциальной информацией, имеющей гриф секретности не выше "Секретно"; 1Б — используется для обработки данных с грифом секретности не выше "Совершенно секретно"; 1А — предназначается для информации с грифом "Особая важность"; 1Г — относится к автоматизированным системам, в которых обрабатывается служебная тайна; 1Д — касается автоматизированных систем, содержащих персональные данные.

7. Сложность выявление инцидента вычисляется по формуле (1): Низкий (Low), Средний (Medium), Высокий (High).

8. Сложность устранения инцидента (Измеряется в часах работы. Каждая компания сама рассчитывает степень сложности устранения инцидента): Низкий (Low), Средний (Medium), Высокий (High).

В классификации указан параметр «Сложность выявления инцидента». Данный параметр можно измерить разными способами: либо измерять в часах, и каждая компания сама решает какая степень сложности выявления инцидента для неё приемлема, либо можно измерить формулой:

$$К1,3 = \sum_i (Wij * Eij) / \sum_i Wij \qquad (1)$$

где E_{ij} - событие i-того запроса в j-той группе, определяемый формулой 2:

$$Eij \begin{cases} 1, \text{ если событие обработано в срок} \\ 1 - \frac{tij}{Ti}, \text{если событие не обработано в срок и } tij \le Ti \\ 0, \text{если событие не обработано в срок и } tij > Ti \end{cases} \qquad (2)$$

а W_{ij} – вес i-того события для j-той группы, определяемый формулой 3:

$$Wij \begin{cases} 1, \text{ если } tij \le Ti \\ \left(\frac{tij}{Ti}\right)^n, \text{если } tij > Ti \end{cases} \qquad (3)$$

В формулах (2)-(3):

- t_{ij} — время, затраченное на обработку i-го события j-й группой;

- T_i — регламентированный максимальный срок обработки i-го события.

Параметр n, как и в формуле (1), является натуральным числом (по умолчанию n=1).

Значение $K_{1,3}$:

Своевременная обработка события: Если событие обработано в срок, коэффициенты E_{ij} и W_{ij} принимают значение 1. Это соответствует низкой сложности выявления инцидента.

Просроченная обработка с превышением полного срока: Если j-я группа затратила на обработку больше времени, чем установленный срок T_i, E_{ij} равен 0, а вес W_{ij} превышает 1 (пропорционально затраченному времени). Это указывает на средний уровень сложности выявления инцидента. Примечание: Группа, исчерпавшая весь выделенный срок, получает снижение метрики $K_{1,3}$ аналогично правилам $K_{1,2}$

Просроченная обработка в рамках половины срока: Если событие просрочено, но j-я группа затратила на обработку, например, половину отведенного времени, E_{ij} равен 0.5, а вес W_{ij} остается равным 1. Это указывает на высокую сложность выявления инцидента.

Также в списке есть пункт «Сложность устранения инцидента». Данный параметр можно измерить только в часах, и каждая компания сама решает какая степень сложности устранения инцидента для неё приемлема. Отдельные инциденты могут быть ликвидированы в разное время с разными затратами. При расчете среднего времени обработки и устранения инцидентов важно учитывать параметр, определяющий установленные компанией нормативы по оптимальным и стандартным срокам их решения. Это происходит из-за того что при анализе инцидентов, помимо оценки показателей $K_{1.1}$-$K_{1.3}$, отражающих соблюдение сроков, необходимо отслеживать динамику среднего времени, затрачиваемого на обработку и закрытие инцидентов. Например, уровень влияния инцидента напрямую связан с регламентированными сроками его устранения, что обуславливает необходимость дифференцированного расчета среднего времени решения для каждого из уровней влияния.

Виды документации для тестирования безопасности информационной инфраструктуры

Степень критичности инцидента ИБ, формат документации об инцидентах, а также регламент тестирования на безопасность информационной инфраструктуры в компании определяются самостоятельно (Методический документ “Руководство по организации процесса управления уязвимостями в органе (организации)” (утв. Федеральной службой по техническому и экспортному контролю 17 мая 2023 г.). В исследовании приведен пример описания карточки инцидента.

Карточка инцидента имеет определенный набор атрибутов. Карточка инцидента сформирована на основе требований описанных в приказах

федеральной службы безопасности (ФСБ) России от 6 мая 2019 г. N 196, приказе ФСБ России от 19 июня 2019 г. N 282, приказе ФСБ России от 19 июня 2019 г. N 281, приказе ФСБ России от 24 июля 2018 г. N 368. В приказах нет рекомендаций по формированию карточки инцидента, но есть требования, на которые необходимо опираться при описании инцидента, чтобы можно было далее его передавать в другие службы, реагировать на него и т.д. Были созданы пункты для описания инцидента:

1. ID - Номер карточки инцидента (Обязательный).
2. Заголовок - С помощью одного предложения описывается суть инцидента. Для написания заголовка используют вопросы “Что? Где? Когда?”. Эти вопросы помогают написать понятный для всех заголовок, не слишком длинный, но отражающий суть инцидента. Пример названия может являться «Превышение количество попыток входа в систему» (Обязательный).
3. Дата, время и географическое местоположение объекта — Указание этих параметров позволяет зафиксировать сведения о месте возникновения компьютерного инцидента, его временных рамках и продолжительности (Обязательный).
4. Причинно-следственная связь — Требуется установить наличие взаимосвязи между компьютерным инцидентом и кибератакой, повлекшей его возникновение. Необходимо описать атаку и описать подробно причину её возникновения (Обязательный).
5. Связь с другими компьютерными инцидентами - Связь с другими компьютерными инцидентами. Привести пример, дату и время инцидента, который ранее возникал в системе (Необязательный).
6. Состав технических параметров системы - Состав технических параметров системы, в которой возник компьютерный инцидент (Обязательный).

7. Последствия - Краткое описание последствий в результате возникновения компьютерного инцидента. Требований к описанию текста нет (Обязательный).

8. Шаги - Описание последовательности действий, которые необходимо выполнить для воспроизведения инцидента. На этом этапе указывается минимум необходимых действий (Обязательный).

9. Фактический результат - Описание полученного результата после выполнения описанных шагов (Обязательный).

10. Ожидаемый результат - Описание результата, который ожидают увидеть после выполнения указанных шагов. Необходимо возобновить инцидент, чтобы выявить всю цепочку его возникновения и выявить все уязвимые места в системе (Обязательный).

11. Серьезность (Компания вырабатывает сама для себя степень серьезности влияния инцидентов на основе материальных затрат для устранения их последствий) - Указывается уровень серьезности влияния инцидента на общую функциональность информационной инфраструктуры или продукта. Критерии: высокий (High), средний (Medium), низкий (Low) (Обязательный).

12. Приоритет - Указывается очередность исправления проблем в результате возникновения инцидента. Высокий (High) — инцидент с таким статусом, будет исправляться в первую очередь. Средний (Medium) — инцидент будет исправляться после всех инцидентов с высоким статусом. Низкий (Low) — инцидент будет исправляться в последнюю очередь, когда все инциденты более высокого приоритета будут исправлены (Обязательный).

13. Вложение - Видео, скриншот, схемы, картинки или логи должны четко демонстрировать выявления инцидента. Можно сделать короткие поясняющие надписи, если это необходимо. При прикреплении вложения в

карточку инцидента необходимо пояснить к какому шагу и пункту относится вложение (Обязательный).

14. Тип инцидента - Исходя из этой информации, можно составить отчет и провести анализ о слабых местах в информационной инфраструктуре продукта, чтобы потом их исправить. Тип инцидента может быть: функциональный, нефункциональный, фатальный, нефатальный, спецификационный, конфигурационный, однозначный, неоднозначный, системный, сегментирующий, потенциальный (Необязательный).

15. Статус - Указывается статус инцидента в его “жизненном цикле”. Статус может быть: новый, дублирующий, закрытый, открытый, отклоненный, отсроченный, переоткрытый (Необязательный).

16. Требование - Указывается ссылка на требование, в котором прописано ожидаемое поведение. Это документация, которая описывается компанией и нормативными документами, которая формируется перед настройкой системы безопасности (Необязательный).

17. Дополнительная информация - Дополнительной информацией может быть файл с тестовыми данными, данные для авторизации и т.д. (Необязательный).

18. Окружение - Необходимо указывать версию продукта, браузера, операционную систему, программного обеспечения и т.д., в которой было обнаружено слабое место в области ИБ (Необязательный).

19. Автор - Указывается человек, который обнаружил и создал карточку инцидента (Необязательный).

20. Исполнитель - Указывается человек, который продолжит работу над исправлением последствий (Необязательный).

21. Комментарии - В комментариях происходит обсуждение инцидента после создания карточки инцидента (Необязательный).

22. Событие - Если ранее в системе было зарегистрировано событие ИБ, и если оно может быть связанно с инцидентом, необходимо указать номер и название события ИБ (Необязательный).

Пример работы атаки и описание инцидента на киберфизическую систему

Для примера описания инцидента была проведена кибератака на экспериментальный стенд КФС - конвейерная лента (рис. 1).

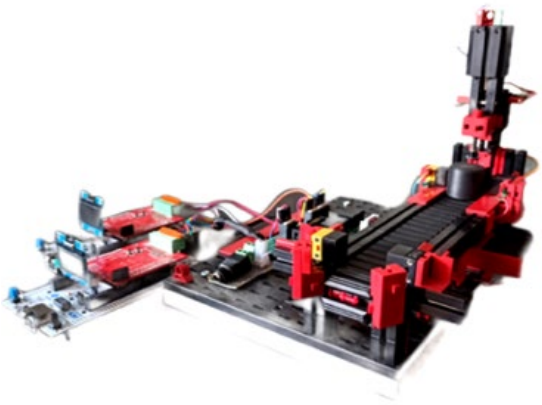

Рис. 1 – Экспериментальный стенд КФС

Стенд состоит из систем человеко-машинного интерфейса (Human-Machine Intelligence - HMI), программно-логического контроллера (Programmable Logic Controller - PLC) и системы диспетчерского управления и сбора данных (supervisory control and data acquisition - SCADA), которые позволяют управлять стендом и считывать с него данные. Также стенд имеет светодиодные датчики, которые определяют порядок действий работы системы. Если реализовать на стенд атаку деаутентификации, то можно нарушить работу стенда, что приведет к застою работы и порчи продуктов, которые стенд может перемещать при своей работе в реальной жизни. Описание инцидента при такой атаке перечислено ниже:

1. ID № 1.
2. Заголовок - Отключение системы от сети.

3. Дата, время и местонахождение объекта - 25.03.2025, г. Таганрог, Ростовская область.

4. Причинно-следственная связь - Стенд был отключен от сети в результате атаки деаутентификации.

5. Связь с другими компьютерными инцидентами - Ранее инцидент не производился.

6. Состав технических характеристик системы - Стенд состоит из систем PLC, HMI, SCADA, данные передаются по протоколу Modbus.

7. Последствия компьютерного инцидента - Стенд был отключен от сети в результате чего он перестал получать команды от управляющего устройства и вышел из строя (перестал перемещать продукты по конвейерной ленте, что привело к их порче).

8. Шаги:

- Необходимо подключиться к сети со стороннего компьютера,

- Выполнить атаку деаутентификации, что приведет к разъединению системы с точкой доступа, и система перестанет получать команды.

9. Фактический результат - Стенд отключился от сети и перестал получать команды от управляющего устройства.

10. Ожидаемый результат - Стенд отключился от сети и перестал получать команды от управляющего устройства.

11. Серьезность - Высокий (High).

12. Приоритет - Высокий (High).

13. Вложение - К карточке инцидента прикреплен лог-файл.

14. Тип инцидента - Функциональный и фатальный.

15. Статус – Новый.

16. Требование - Необходимо проверить систему безопасности точки доступа, чтобы злоумышленник не мог к ней подключиться.

17. Дополнительная информация - Описание работы точки доступа и инструкция как к ней подключиться.

18. Окружение - Роутер фирмы АБВГД номер 12345.

19. Автор - Иван Иванов Иванович.

20. Исполнитель - Петр Иванов Иванович.

21. Событие - Ранее были получены логи о том, что хост с ip-адресом 192.168.1.1 пытался подключиться к сети.

Заключение

Киберфизические системы – это сложные ИС, которые собирают данные с окружающей среды, обрабатывают их и передают дальше комплексу устройств и датчиков для выполнения тех или иных функций, которые зависят от полученных данных. В таких системах может быть внедрен ИИ, алгоритмы обнаружения информационных угроз и защиты от них. Информационные атаки могут критически влиять на процессы работы таких систем, поэтому очень важно вовремя реагировать на компьютерные инциденты и избегать риски их появления. Для этого необходимо настраивать системы мониторинга для выявления аномальной работы: повышение нагрузки системы, проникновение в систему, сканирование системы, появление в трафике неизвестных пакетов и тд. [8 - 10].

Рекомендации в этой работе по описанию инцидента КФС улучшат обеспечение безопасности таких систем. Поставленные цели и задачи были выполнены в данной работе, были проанализированы компьютерные инциденты, выявлены причины их возникновения, разработаны рекомендации по устранению нарушений, а также рекомендации по описанию компьютерных инцидентов при тестировании безопасности КФС.

Литература

1. Ротанов Е.Г., Шаховской А.В., Соколов И.В. Перспективы развития систем промышленной автоматизации в контексте индустрии 4.0 // Инженерный вестник Дона, 2025, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9972.

2. Mikhailova V.D., Shulika M.G., Basan E.S., and Peskova O.Y. (2021, January 13-14). Security architecture for UAV. Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia. DOI: 10.1109/USBEREIT51232.2021.9455039 EDN: DSQEHP.

3. Basan E., Basan A., Nekrasov A., "Method for detecting abnormal activity in a group of mobile robots," Sensors 2019, 19(18):4007, pp. 1-21, DOI: 10.3390/s19184007

4. Басан А.С., Басан Е.С., Иванникова Т.Н., Корчаловский С.В., Михайлова В.Д., Шулика М.Г. Концепция базы знаний угроз киберфизических систем на основе онтологического подхода // Системный синтез и прикладная синергетика: Сборник научных работ XI Всероссийской научной конференции, п. Нижний Архыз, 27 сентября – 01 января 2022 года. – Ростов-на-Дону - Таганрог: Южный федеральный университет, 2022. – С. 172-177. – DOI: 10.18522/syssyn-2022-33. – EDN UHQKZZ.

5. Бутусов И.В., Романов А.А. Предупреждение инцидентов информационной безопасности в автоматизированных информационных системах // Вопросы кибербезопасности. – 2020. – № 5(39). – С. 45-51. – DOI: 10.21681/2311-3456-2020-05-45-51. – EDN IWBAQR.

6. Макарова А.К., Макеев Н.А. Сравнение подходов к расследованию кибер инцидентов в России и зарубежных странах // Вестник науки и образования Северо-Запада России. – 2023. – Т. 9, № 3. – С. 84-89. – EDN COTGYU.

7. Крюков Д. М. Графоаналитическая модель процесса ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты // Инженерный вестник Дона, 2022, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7613.

8. Basan E., Basan A., Makarevich O., Babenko L. Studying the impact of active network attacks on a mobile robots group // Voprosy kiberbezopasnosti, 2019, №1, pp.35-44, ISSN 2311-3456. DOI: 10.21681/2311-3456-2019-1-35-44.

9. Statt Nick, Skydio's AI-Powered Autonomous R1 Drone Follows You Around in 4K // TheVerge – URL: theverge.com/2018/2/13/17006010/skydio-r1-autonomousdrone-4k-video-recording-ai-computer-vision-mapping.

10. Басан Е.С., Михайлова В.Д., Шулика М.Г., Лесников А.А., Могильный А.Б. Определение набора метрик для детектирования атак на КФС // Системный синтез и прикладная синергетика: Сборник научных работ XI Всероссийской научной конференции, п. Нижний Архыз, 27 сентября – 01 января 2022 года. – Ростов-на-Дону - Таганрог: Южный федеральный университет, 2022. – С. 183-189. – DOI: 10.18522/syssyn-2022-35. – EDN OQMHSK.

References

1. Rotanov E.G., Shaxovskoj A.V., Sokolov I.V. Inzhenernyj vestnik Dona, 2025, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9972.

2. Mikhailova V.D., Shulika M.G., Basan E.S., and Peskova O.Y. (2021, January 13-14). Security architecture for UAV. Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia. DOI: 10.1109/USBEREIT51232.2021.9455039 EDN: DSQEHP.

3. Basan E., Basan A., Nekrasov A., "Method for detecting abnormal activity in a group of mobile robots," Sensors 2019, 19(18):4007, pp. 1-21, DOI: 10.3390/s19184007

4. Basan A.S., Basan E.S., Ivannikova T.N., Korchalovskij S.V., Mixajlova V.D., Shulika M.G. Sistemny`j sintez i prikladnaya sinergetika: Sbornik nauchny`x rabot XI Vserossijskoj nauchnoj konferencii, 27 sentyabrya – 01 yanvarya 2022 goda. Rostov-na-Donu - Taganrog: Yuzhnyj federal'nyj universitet, 2022. pp. 172-177. DOI: 10.18522/syssyn-2022-33. EDN UHQKZZ.

5. Butusov I.V., Romanov A.A. Voprosy` kiberbezopasnosti. 2020. № 5(39). pp. 45-51. DOI: 10.21681/2311-3456-2020-05-45-51. EDN IWBAQR.

6. Makarova A.K., Makeev N.A. Vestnik nauki i obrazovaniya Severo-Zapada Rossii. 2023. T. 9, № 3. pp. 84-89. EDN COTGYU.

7. Kryukov D. M. Inzhenernyj vestnik Dona, 2022, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2022/7613.

8. Basan E., Basan A., Makarevich O., Babenko L., Voprosy kiberbezopasnosti, 2019, №1. Pp.35-44. ISSN 2311-3456. DOI: 10.21681/2311-3456-2019-1-35-44.

9. Statt Nick Skydio's AI-Powered Autonomous R1 Drone Follows You Around in 4K. TheVerge. URL: theverge.com/2018/2/13/17006010/skydio-r1-autonomousdrone-4k-video-recording-ai-computer-vision-mapping.

10. Basan E.S., Mixajlova V.D., Shulika M.G., Lesnikov A.A., Mogil`ny`j A.B. Sistemnyj sintez i prikladnaya sinergetika: Sbornik nauchnyh rabot XI Vserossijskoj nauchnoj konferencii, p. Nizhnij Arhyz, 27 sentyabrya – 01 yanvarya 2022 goda. Rostov-na-Donu - Taganrog: Yuzhnyj federal'nyj universitet, 2022. pp. 183-189. DOI: 10.18522/syssyn-2022-35. EDN OQMHSK.

Дата поступления: 13.04.25

Дата публикации: 25.05.25