Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры

Н.В. Кучкарова
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: nailya_kuchkarov@mail.ru

В.И. Васильев
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: vasilyev@ugatu.ac.ru

А.М. Вульфин
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет Уфа, Россия
e-mail: vulfin.alexey@gmail.com

Аннотация[1]

Одной из актуальных задач, возникающих при определении защищенности систем автоматизированного управления (АСУ) технологическими процессами (ТП) и производствами, является задача оперативного поиска и определения перечня уязвимостей. В статье описывается подход к определению актуальных уязвимостей современных АСУ ТП. Проводится краткий анализ существующей нормативно-правовой базы обеспечения информационной АСУ ТП на критически важных объектах. Рассмотрены различные варианты классификации уязвимостей. Проведен сравнительный анализ существующих открытых баз данных уязвимостей.

1. Введение

По словам известного интернет-издания РБК,: «Эксперты Всемирного экономического форума (ВЭФ) назвали кибератаки, достигшие «беспрецедентных масштабов», одними из главных глобальных рисков после экологических и геополитических проблем. Пока кибератакам отведено шестое место в десятке технологических рисков. Но не пройдет и пяти лет, как эта угроза может занять первую строчку» (15 марта 2018г). В последние годы неуклонно растет количество кибератак на промышленные объекты [1]. Обеспечение защищенности значимых объектов критической информационной инфраструктуры (КИИ) сегодня является одной из важнейших задач, решаемых специалистами по информационной безопасности. Это связано с тем, что промышленные предприятия нефтеперерабатывающей, энергетической и других отраслей представляют серьезную потенциальную опасность: экологическую, финансовую, не говоря уже о прямой угрозе жизни и здоровья населения целых регионов. Для промышленных объектов при этом характерны уязвимости как информационных систем (ИС), так и компонентов АСУ ТП. Рост уязвимостей обусловлен появлением новых видов программного обеспечения (ПО). Большое количество информации, связанное с обнаруженными уязвимостями, потребовало унифицированного подхода к их обработке. К сожалению, на данный момент в различных базах данных уязвимостей используются различные способы систематизации такой информации. Хотя основные характеристики уязвимости, такие как наименование операционной системы (ОС) и тип аппаратной платформы, наименование ПО и его версия, степень опасности уязвимости, содержатся во многих из них. Обеспечение безопасности промышленной сети и АСУ ТП требует комплексного подхода, учитывающего особенности промышленных систем и основанного на требованиях и рекомендациях как международных стандартов, так и российских нормативных документов по обеспечению информационной безопасности промышленных систем. К таким документам относятся приказы ФСТЭК России №31,

Труды Седьмой Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений», 28-30 мая, Уфа-Ставрополь-Ханты-Мансийск, Россия, 2019

№239, а также ГОСТы серии 62443 и 56545, определяющие требования к обеспечению защиты информации в АСУ ТП.

2. Краткий анализ стандартов серий 62443, 56545 и приказов ФСТЭК

- Первые стандарты серии 62443 введены на территории Российской Федерации в 2016 году, они являются русскоязычными версиями соответствующих международных стандартов IEC/TC 62443. В настоящий момент переведено 3 документа из этой серии. Далее рассмотрим области применения и некоторые особенности каждого из них:

- ГОСТ Р 56205-2014 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (IEC/TS 62443-1-1:2009 Industrial communication networks. Network and system security. Part 1-1. Terminology, concepts and models). Относится к общим стандартам этой серии. Объектом являются системы промышленной автоматики и контроля (IACS), включающие в себя системы управления (распределенные системы управления, программируемые логические контроллеры, пульты дистанционного управления, системы диспетчерского контроля и сбора данных (SCADA) и т.д.). Стандарт устанавливает единую терминологию, базовые концепции (цели безопасности, требования к безопасности IACS, политики безопасности и т.д.) и описывает модели (базовые, объектные, зональная, базовую архитектуру), необходимые для разработки программы безопасности [2];

- ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. (IEC 62443-2-1:2010. Industrial communication networks. Network and system security. Part 2-1. Establishing an industrial automation and control system security program. Данный стандарт включает в себя описание компонентов системы управления кибербезопасностью (CSMS) для IACS, приводятся указания по разработке CSMS для IACS. Содержит справочные приложения. В Приложении А, в частности, содержится руководство по разработке элементов системы управления кибербезопасностью, описывающее общую концепцию системы управления, которую можно адаптировать под требования конкретного предприятия [3];

- ГОСТ Р МЭК 62443-3-3—2016 Сети коммуникационные промышленные. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности. Industrial communication networks. Network and system security. Part 3-3. System security requirements and security levels. Относится к системным стандартам этой серии. В документе сформулированы системные требования к системам управления, привязанные к семи фундаментальным требованиям (FR) (управление идентификацией и аутентификацией, контроль использования, целостность системы, конфиденциальность данных, ограничение потока данных, своевременный отклик на события, работоспособность и доступность ресурсов [4].

- Стандарты серии 56545 определяют общие требования к структуре описания и классификации уязвимостей:

- ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей». Стандарт устанавливает общие требования к структуре описания уязвимости и правила описания уязвимости ИС. Предлагается форма паспорта уязвимости с примером его заполнения [5];

- ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». Стандарт устанавливает классификацию уязвимостей ИС [6].

- Для специалистов в области информационной безопасности ИБ представляют интерес также приказы ФСТЭК России, устанавливающие нормативные требования к обеспечению безопасности АСУ ТП:

- Приказ ФСТЭК России №31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». В документе предлагается разделение АСУ на три уровня: 1) уровень операторского (диспетчерского управления) (SCADA, коммутаторы, маршрутизаторы); 2) уровень автоматического управления (промышленная сеть передачи данных, контроллеры и т.д.); 3) уровень ввода (вывода) данных исполнительных устройств (датчики, промышленные механизмы и т.д.) Определение угроз безопасности информации осуществляется на каждом из уровней системы управления и состоит из

четырех обязательных этапов: 1) выявление источников угроз безопасности информации; 2) анализ возможных уязвимостей АСУ ТП; 3) определение возможных способов реализации угроз безопасности; 4) оценка возможных последствий [7];

- Приказ ФСТЭК России № 239 от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации». В этом документе даются рекомендации по обеспечению безопасности значимых объектов на различных стадиях их жизненного цикла:
- а) установление требований к обеспечению безопасности значимого объекта;
- б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;
- в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;
- г) обеспечение безопасности значимого объекта в ходе его эксплуатации;
- д) обеспечение безопасности значимого объекта при выводе его из эксплуатации. [8]
- Задание требований к обеспечению безопасности значимых объектов безопасности устанавливается в соответствии с категорией значимости значимого объекта. Процесс создания подсистемы безопасности значимого объекта должен включать:
- а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);
- б) проектирование подсистемы безопасности значимого объекта;
- в) разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).
- Анализ угроз безопасности информации должен включать:
- а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
- б) анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
- в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
- г) оценку возможных последствий от реализации (возникновения) угроз безопасности информации.
- В качестве исходных данных для анализа угроз безопасности информации при этом необходимо использовать банк данных угроз безопасности ФСТЭК России и источники, содержащие иные сведения об угрозах безопасности информации. Результат анализа должен подтверждать тот факт, что в объекте отсутствуют угрозы, содержащиеся, как минимум, в банке данных угроз ФСТЭК

3. Классификация уязвимостей в информационных системах

Попытки классифицировать уязвимости и угрозы предпринимались с момента возникновения необходимости создания безопасных информационных систем. В настоящий момент существуют различные способы классификации уязвимостей автоматизированных систем (АС). Рассмотрим некоторые из них:

по типу обеспечения АС, в котором содержится уязвимость (уязвимость аппаратного обеспечения, уязвимость общесистемного программного обеспечения, уязвимость прикладного программного обеспечения);

по типу компонента АС, в котором содержится уязвимость (уязвимость рабочих станций, уязвимость серверов АС, уязвимость коммуникационного оборудования и каналов связи АС);

по типу жизненного цикла АС, на котором внедрялась уязвимость (уязвимость технологического этапа, уязвимость эксплуатационного этапа);

по степени преднамеренности внесенной уязвимости АС (уязвимость, внесенная преднамеренным путем, уязвимость, внесенная непреднамеренным путем);

по уровню модели сетевого взаимодействия, на котором присутствует уязвимость (уязвимость физического уровня, уязвимость канального уровня, уязвимость сетевого уровня, уязвимость транспортного уровня, уязвимость прикладного уровня).

Следующий вариант классификации:

по уровню информационной структуры организации. К уровню сети относятся уязвимости сетевых протоколов: стека TCP/IP, NetBEUI, IPX/SPX. Уровень операционной системы охватывает уязвимости Windows, UNIX, Novell и т.д. Уязвимости баз данных: Oracle, MSSQL, Sybase. Также существуют классификации уязвимости по степени риска (высокий, средний, низкий).

Специалисты в области информационной безопасности АСУ ТП используют специальные базы данных (классификаторы) уязвимостей.

Сравнительный анализ наиболее известных баз уязвимостей CVE (Common Vulnerabilities and Exposures) и NVD (National Vulnerability Database) (OSVDB была закрыта разработчиками в 2016 г.) был дан в работах [9, 10]. Используя для анализа критерии, предложенные авторами этих статей, проанализируем некоторые базы уязвимостей. ICS-CERT (Национальный центр интеграции кибербезопасности и связи (NCCIC)) Структура записей сходна с записями в базе NVD. Также содержит показатели метрики общей системы оценки уязвимостей (Common Vulnerability Scoring System, CVSS). NCCIC является спонсором NVD - хранилища данных управления уязвимостями, основанного на стандартах правительства США.

Secunia Advisory and Vulnerability Database (Secunia). Структура записей в базе Secunia сходна с записями в базе NVD. Положительные стороны - для этой базы характерно наличие информации о множестве отдельных уязвимостей, одновременно обнаруженных в одном и том же программном обеспечении. Недостатки - не всегда присутствует CVE-идентификатор, бесплатное скачивание доступно только в формате html.

База VND от CERT/CC (Vulnerability Notes Database). Положительные стороны - записи в базе VND содержат подробное и детальное руководство по устранению уязвимостей и/или предотвращению их эксплуатации злоумышленником, возможность полного скачивания всех записей базы в формате JSON с помощью специального бесплатно предоставляемого программного обеспечения, использует метрики CVSS. Недостатки – не всегда присутствует CVE-идентификатор, редкое обновление базы (несколько раз в месяц).

С марта 2015г. в России функционирует банк данных угроз безопасности информации данных Федеральной службы по техническому и экспортному контролю (ФСТЭК). Данный реестр в первую очередь ориентирован на сбор и хранение информации об угрозах и уязвимостях ПО, используемого в государственных организациях Российской Федерации, включая информационные системы и системы управления критичными производственными процессами. Эта система содержит 5 фильтров для поиска угроз и более 15 – для поиска уязвимостей. Используются метрики CVSS, рекомендации по устранению угроз (уязвимостей), ссылки на идентификаторы других систем уязвимости и др.

При таком многообразии баз данных уязвимостей, для качественного обеспечения информационной безопасности АСУ ТП необходимо проанализировать большое количество информации «вручную», что, по понятным причинам, сделать достаточно сложно. В этом ключе, вполне закономерно появление агрегаторов информации о уязвимостях, таких как CVE Details, который собирает всю доступную из публичных реестров и баз уязвимостей информацию по конкретному CVE-идентификатору и объединяет ее в единую запись. Или Vulners – поисковая система со своей базой уязвимостей. Этот сайт также содержит сканер уязвимостей, инструмент для оценки уязвимостей (нейронные сети), позволяет импортировать API [11].

Некоторые из приведенных баз уязвимостей используют показатели метрики CVSS. Это инструментарий для расчета числового показателя по десятибалльной шкале, который позволяет специалистам по информационной безопасности определить, насколько критична та или иная уязвимость. Чем выше значение метрики, тем опаснее уязвимость. Существуют базовые, временные, контекстные метрики.

Проблема раскрытия информации об уязвимостях возникла давно. Для упорядочения обработки и согласованного управления информацией была создана рабочая группа по раскрытию информации о уязвимостях - Vulnerability Disclosure Framework (VDF). Согласно документу, выпущенному этой группой, жизненный цикл уязвимостей состоит из девяти этапов:

1. Исследование, результатом которого является превращение теоретической возможности совершить атаку через какую-либо «дыру», в реальность, воплощенную в т.н. эксплоите (exploit);

2. Проверка позволяет удостовериться, что уязвимость – это не случайный результат функционирования системы, а свойство, которым можно воспользоваться в любой момент;

3. Уведомление владельца уязвимой системы, которое осуществляется с ним напрямую или через координатора;

4. Оценка владельца уязвимой системы позволяет подтвердить выводы исследователя;

5. Подтверждение является результатом положительной оценки и сигналом исследователю, что владелец будет поддерживать с ним дальнейший контакт для будущих исследований и обсуждения плана раскрытия информации;

6. Устранение заключается в разработке рекомендаций или патча для обнаруженной уязвимости.

7. Тестирование рекомендаций и патча подтверждает, что они негативно не повлияют на работу системы и ее окружения;

8. Выпуск патча и рекомендаций делает их доступными для пользователей;

9. Обратная связь и закрытие задачи;

Не всегда уязвимости проходят все девять этапов. Их судьба зависит от участников процесса, занятых в управлении уязвимостями.

4. Определение уязвимостей сетевого компонента АСУ ТП в соответствии с ГОСТ Р МЭК 62443-2-1-2015

В этом документе предлагается идентифицировать и проверить следующие потенциальные источники уязвимостей:

- точки беспроводного доступа, особенно в случае применения плохо защищенных технологий, например, ранние версии IEEE 802.11;
- ПО для дистанционного доступа (например, pcAnywhere и Timbuktu), обычно применяющиеся для доступа специалистов внутри организации или за ее пределами для поддержки систем или операций. Такие приложения обеспечивают достаточный контроль и доступ к конфигурированию для неавторизованного лица;
- любые сетевые подключения к системе, не являющиеся непосредственным компонентом IACS;
- технологии дистанционной работы с окнами, например, X Windows;
- модемные соединения, особенно без посылки обратного вызова и не предусматривающие шифрование;
- внутренние сетевые соединения;
- соединения Интернет;
- телеметрические сети;
- любые сетевые соединения, используемые для сопряжения компонентов SCADA или системы управления, которые не являются частью специальной физически защищенной сети IACS.

В соответствии с ГОСТом результатом работы группы специалистов по информационной безопасности «…является список уязвимостей, расставленных в порядке приоритета с учетом их влияния на риск. После идентификации уязвимостей группа связывает их с угрозами, последствиями и прочими вероятными результатами реализации угрозы и уязвимости».

5. Вывод

Принимая во внимание проведенный выше анализ требований нормативной документации и особенностей баз данных уязвимостей, можно сделать вывод о том, что для обеспечения адекватного анализа уязвимостей АСУ ТП значимых объектов критической информационной инфраструктуры, специалистам по информационной безопасности, в первую очередь, необходимо учитывать уязвимости, содержащиеся в банке данных угроз и уязвимостей ФСТЭК. Для более эффективного (во временном и количественном отношении) мониторинга наличия уязвимостей на предприятиях КИИ целесообразно использовать агрегаторы такие как, CVE Detail или Vulners. Результаты анализа позволят оценить защищенности АСУ ТП, провести оценку рисков информационной безопасности и выбрать необходимый набор контрмер по защите информации.

Acknowledgments (благодарности)

Работа выполнена при поддержке гранта РФФИ № 17-07-00351-А-07-396.

Список используемых источников

1. Кибератаки на критическую инфраструктуру — миф или реальность? [Электронный ресурс]. – Режим доступа: http://www.jetinfo.ru/stati/kiberataki-na-kriticheskuyu-infrastrukturu-mif-ili-realnost. (дата обращения 14.02.2019).
2. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200114169 (дата обращения 07.02.2019).
3. ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2) Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200121982 (дата обращения 07.02.2019).
4. ГОСТ Р 56498 IEC 62443-3-3-2016 Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru /document/1200135801 (дата обращения 07.02.2019).
5. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – М.: Стандартинформ, 2015. -12 с.
6. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – М.: Стандартинформ, 2015. -12 с.
7. Приказ ФСТЭК России от 14.03.2014 № 31 [Электронный ресурс]. – Режим доступа: https://www.law.ru/npd/doc/docid/420397221/modid/99 (дата обращения 07.02.2019).

8. Приказ ФСТЭК от 25.12.2017 № 239 “Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации” [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/ipo/prime/doc/71801880/ (дата обращения 07.02.2019).
9. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Научно-практическая конференция «РусКрипто’2014». - Москва: Изд-во Карат, 2014. — 17 с.
10. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы уязвимостей // Изв. ВУЗов. Приборостроение. - 2014.-№11. Т.57. С.62-67.
11. Vulners — Гугл для хакера. Как устроен лучший поисковик по уязвимостям и как им пользоваться. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/xakep/blog/305262/ (дата обращения 21.02.2019).