ПИНУС А. С., БАЗАРОВА И. А., ХОЗЯИНОВА Т. В. ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА УЯЗВИМОСТЕЙ ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

УДК 002:025.2/3, ВАК 05.13.01, 20.17.17

Информационная система учета уязвимостей оборудования и программного обеспечения автоматизированных систем управления технологическим процессом

А. С. Пинус, И. А. Базарова, Т. В. Хозяинова

Ухтинский государственный технический университет, г. Ухта

Информационная система учета уязвимостей оборудования и программного обеспечения автоматизированных систем управления технологическим процессом.

В статье рассматривается информационная система учета уязвимостей оборудования и программного обеспечения автоматизированных систем управления технологическим процессом. В данной статье поднимаются вопросы учета уязвимостей оборудования и программного обеспечения эксплуатируемого на предприятии, а также составления различного вида отчетностей.

Ключевые слова: *информационная система, систему учета, учет уязвимостей, ASP.NET.*

Information system for recording equipment and software vulnerabilities of automated process control systems

A. S. Pinus, I. A. Bazarova, T. V. Khozyainova

Ukhta State Technical University, Ukhta

Information system of accounting of vulnerabilities of equipment and software of automated process control systems.

The article deals with the information system of accounting vulnerabilities of equipment and software of automated process control systems. This article raises the issues of accounting for vulnerabilities of equipment and software used in the enterprise, as well as the preparation of various types of reports.

Keywords: *information system, accounting system, vulnerability accounting, ASP.NET*

Введение

В составе АО «Транснефть – Север» до 31.01.2019 года находился Инженерный центр Автоматизированных систем управления технологическим процессом (далее АСУТП), подразделение, основной задачей которого было создание АСУТП решений для организаций системы «Транснефть» (далее ОСТ). Со-

временные АСУТП это сложные многокомпонентные системы, работающие в составе распределенных сетевых инфраструктур. Кибератаки на такие системы обладают большим разрушительным потенциалом и способны повлечь за собой масштабные экологические, социальные и экономические последствия. Поэтому одно из подразделений Инженерного центра АСУТП – Отдел анализа защищенности АСУТП – было нацелено на разработку решений информационной безопасности АСУТП.

Одним из направлений деятельности отдела был мониторинг уязвимостей программного обеспечения (далее ПО) и оборудования АСУТП. Мониторинг уязвимостей ПО и оборудования – это процесс обнаружения в открытых источниках и учета уязвимостей ПО и оборудования, находящегося в составе эксплуатируемых в ОСТ МПСА (микропроцессорная система автоматизации). Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности информации. С учетом широкого распространения, тиражируемого ПО, процесс управления уязвимостями каждого отдельного предприятия должен быть организован с опорой на централизованный систематический процесс обнаружения и учета уязвимостей. Такой процесс ведется компанией MITRE – некоммерческой организацией, специализирующейся в области системной инженерии, в рамках проекта CVE (Common Vulnerabilities and Exposures), стартовавшего в 1999 году. В рамках процесса выпускается пополняемый реестр зарегистрированных уязвимостей ПО и оборудования, в котором каждая уязвимость идентифицируется уникальным идентификатором – CVE, имеющий вид CVE – год – порядковый номер. Например, CVE-2019-12515).

Единицей учета уязвимостей в интересах обеспечения информационной безопасности предприятия является не любая обнаруженная уязвимость из реестра CVE, а уязвимость, способная привести к актуальной угрозе в соответствии с моделью угроз, действующей на предприятии [1]. Иными словами, актуальная уязвимость, относящаяся к программному обеспечению и оборудованию, находящемуся в эксплуатации на предприятии. С целью накопления информации об известных уязвимостях ПО и оборудования, в процессе мониторинга фиксируется полная информация обо всех опубликованных уязвимостях, даже если это ПО или оборудование на текущий момент не применяется в АСУТП ОСТ. В процессе мониторинга регистрируется более чем 20 характеристик, которые позволяют сделать вывод об опасности уязвимости в случае реализации угрозы [2]. При этом данные об уязвимостях постоянно обновляются и пополняются, поэтому в процессе мониторинга важно не только обнаружить и регистрировать новые актуальные уязвимости, но и отслеживать изменения, которые произошли с характеристиками уязвимостей, зарегистрированных ранее.

Целью работы является создание информационной системы учёта уязвимостей оборудования и программного обеспечения АСУТП.

Система должна выполнять следующие функции:

1) учет уязвимости и её характеристик;

2) поиск уязвимостей по характеристикам;

3) формирование еженедельного отчета о зарегистрированных уязвимостях;

4) формирование статистического отчета о зарегистрированных уязвимостях за период времени;

5) импорт данных об уязвимостях из базы данных (далее БД) NIST NVD [3, 4].

Предпроектное обследование

Уязвимость информационной системы – недостаток или слабое место в системном или прикладном программном обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности информации.

Обнаружением уязвимости могут заниматься:

1. Компании, производящие ПО – при производстве и тестировании ПО, может появляться информация о различных видах уязвимости продукта, которые в дальнейшем нужно будет исправить.

2. Компании, использующие ПО – при наличии отдела в компании, который занимается мониторингом ПО, задействованного на предприятии, в ходе эксплуатации ПО, могут обнаружится уязвимости, о которых будет нужно сообщить.

3. Свободные организации, занимающиеся поиском уязвимостей – организации, цель которых обнаружить уязвимость в ПО и сообщить о таковой.

На данный момент многие злоумышленники фокусируют свои усилия именно на обнаружении уязвимостей в программном обеспечении. Это обусловлено высокой эффективностью использования уязвимостей, что, в свою очередь, связано с двумя фактами – высоким распространением уязвимого ПО и некоторым временным промежутком между обнаружением уязвимости компанией-разработчиком программного обеспечения и выпуском соответствующего обновления для исправления ошибки.

Именно поэтому своевременная публикация уязвимостей так необходима. О найденных уязвимостях сообщают в специализированные организации, носящие название CNA – CVENumberingAuthority, которые в свою очередь подтверждают наличие данной уязвимости. CNA – это организации со всего мира, которым разрешено назначать CVE ID уязвимостям, в согласованных за ними областях, и включать эту информацию в объявления об обнаружении новых уязвимостей.

Подтверждением уязвимости и регистрацией занимается Primary CNA – MITRE [3]. MITRE – американская некоммерческая организация, базирующаяся в штате Вирджиния. Именно MITRE взяла на себя обязанность систематизировать, и регистрировать уязвимости, с целью дальнейшей публикации. MITRE занимается поддержкой базы данных CVE (Common Vulnerabilities and Exposures) – база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

После регистрации уязвимости в базе данных CVE, уязвимость необходимо оценить. Оценкой уязвимости занимается организация NIST, используя общую систему оценки уязвимости (CVSS). Используя CVSS, NIST присваивает оценку уязвимости и публикует это в своей базе данных NIST National Vulnerability Database [4]. Помимо первичной публикации оцененной уязвимости NIST публикует обновления по уязвимостям, с произведенной при необходимости повторной оценкой, вызванной изменением в ПО. Это помогает отслеживать изменение угрозы от уязвимости, и реагировать на нее.

Объектом автоматизации является процесс мониторинга уязвимостей ПО и оборудования АСУТП.

В составе АО «Транснефть-Север» до 31.01.2019 года находился Инженерный центр АСУТП, подразделение, основной задачей которого было создание АСУТП решений для организаций системы «Транснефть». Современные автоматизированные системы управления технологическим процессом это сложные многокомпонентные системы, работающие в составе распределенных сетевых инфраструктур. Кибератаки на такие системы обладают большим разрушительным потенциалом и способны повлечь за собой масштабные экологические, социальные и экономические последствия. Поэтому одно из подразделений Инженерного центра АСУТП – Отдел анализа защищенности АСУТП – было нацелено на разработку решений по информационной безопасности АСУТП.

Основными функциями данного отдела являются:

1. Организация учёта всего ПО, используемого на объектах ПАО «Транснефть».
2. Глубокий анализ решений по реализации защищенности используемого ПО.
3. Контроль изменений в используемом ПО.
4. Оповещение ОСТ, использующих ПО, о выходе новых версий, с целью его обновления на объектах.
5. Мониторинг и регистрация уязвимостей.

Мониторинг и регистрация уязвимостей является важным рабочим процессом в отделе анализа защищённости.

Этот процесс состоит из следующих этапов.

1. Ответственный сотрудник отдела изучает источники информации о зарегистрированных уязвимостях с целью выявления новых зарегистрированных уязвимостей.
2. Ответственный сотрудник отдела определяет насколько актуальна уязвимость для ОСТ, используя внутренние источники данных о составе эксплуатируемых АСУТП.
3. Ответственный сотрудник отдела регистрирует уязвимость.
4. Ответственный сотрудник отдела выпускает необходимую отчетность о зарегистрированных уязвимостях.

Для каждой из зарегистрированных уязвимостей, критичность которой превышает определенное значение вырабатывается решение о мерах по реаги-

рованию с целью устранения уязвимости или предотвращения возможности ее эксплуатации.

Для поиска сведений о применении уязвимого ПО на предприятии ПАО «Транснефть» используется АССО ПТО.

АССО ПТО – это система учета единиц оборудования и программного обеспечения, используемого на предприятии.

Уязвимость вносится в специальный реестр, который на момент начала работы над ВКР велся в формате Excel. Мониторинг источников уязвимости осуществляется при помощи АССО и группы источников информации об уязвимостях.

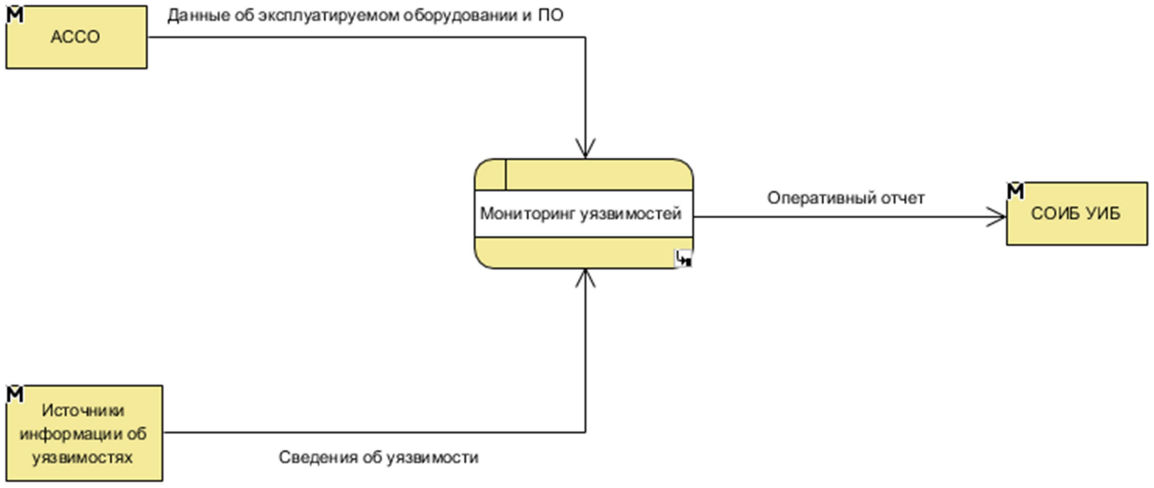

Рисунок 1 – Контекстная диаграмма процесса «как было»

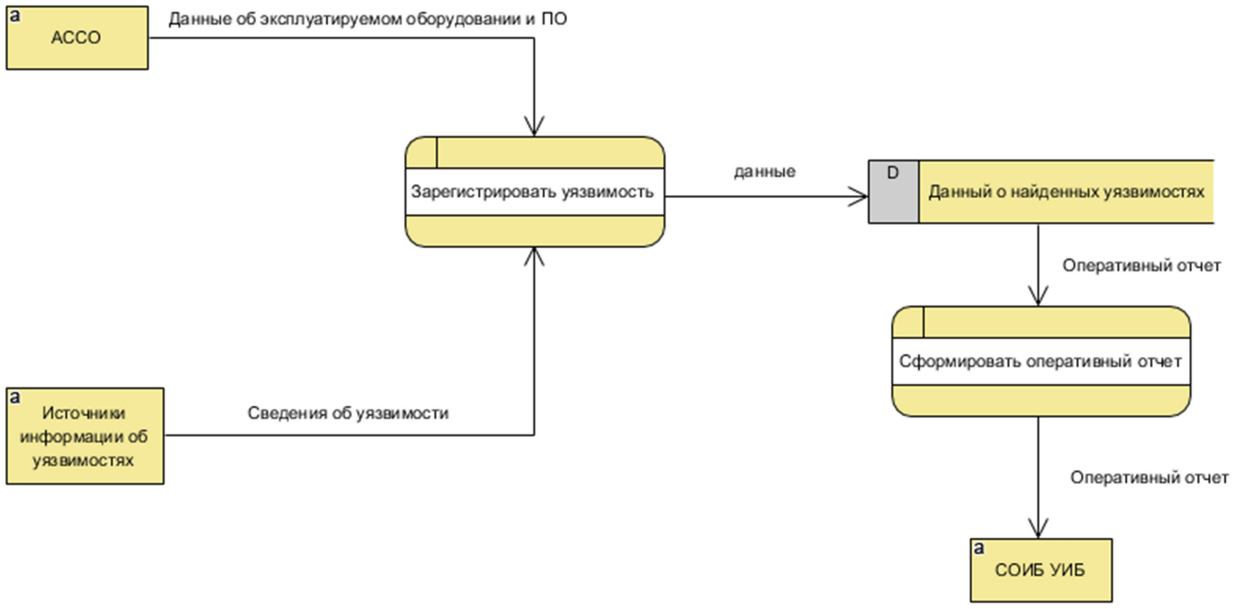

Рисунок 2 – Декомпозиция процесса

Недостатки такой организации процесса в существенной трудоемкости регистрации уязвимости и ее характеристик без опоры на актуальный автоматизированный источник данных об уязвимостях (каким, например, является NIST

NVD), а также отсутствии процессов, связанных с ретроспективой зарегистрированных ранее уязвимостей, с целью получения сведений об изменении характеристик. Также в связи с отсутствием автоматизации процесса выпуск необходимой отчетности для СОИБ УИБ не был возможен, выпускался единственный еженедельный бюллетень.

Поэтому было принято решение о внесении изменений в процесс и его автоматизации. Первоначальные данные об уязвимостях должны поступать из общедоступной БД уязвимостей (NIST NVD). Источники служат для пополнения сведений об уязвимости, а в определенных случаях получения первоначальных сведений.

В ходе работы были выявлены следующие функциональные требования к системе:

1. Учет уязвимости и её характеристик.
   - 1.1. При учете уязвимости система должна предоставлять возможность регистрировать следующие ее параметры:
     - 1.1.1. CVE id.
     - 1.1.2. Описание уязвимости.
     - 1.1.3. Поставщик оборудования или ПО.
     - 1.1.4. Продукт подверженный уязвимости.
     - 1.1.5. Версия продукта, подверженного уязвимости.
     - 1.1.6. Дата публикации уязвимости.
     - 1.1.7. Критичность атаки.
     - 1.1.8. Вектор атаки.
     - 1.1.9. Сложность доступа.
     - 1.1.10. Решение по уязвимости.
     - 1.1.11. Ссылки на источники информации.
     - 1.1.12. Дата выпуска ТСБ.
     - 1.1.13. Ссылка на ТСБ.
   - 1.2. Система должна проверять номер уязвимости CVE на уникальность при регистрации новой уязвимости.
   - 1.3. Система должна предоставлять возможность пополнять справочники производителей, программного обеспечения, версий программного обеспечения непосредственно в процессе регистрации уязвимостей, если необходимый элемент отсутствует в справочнике.
   - 1.4. При регистрации новых элементов в справочнике система должна осуществлять проверку наименования элемента на уникальность.
   - 1.5. Система должна предоставлять возможность редакции уязвимости.
2. Поиск уязвимости по характеристикам.
   - 2.1. Система должна предоставлять возможность поиска уязвимости по следующим ее характеристикам:
     - 2.1.1. CVE id.
     - 2.1.2. ПО и оборудование.

2.1.3. Место эксплуатации уязвимости (ОСТ).

3. Формирование еженедельного отчета о зарегистрированных уязвимостях.
4. Формирование статистического отчета о зарегистрированных уязвимостях за определенный период времени.
   4.1. В состав отчета должны входить следующие данные:
      4.1.1. количество выявленных уязвимостей по критичности за промежуточные периоды времени в табличном и графическом виде;
      4.1.2. количество уязвимостей по источникам (в табличном и графическом виде);
      4.1.3. данные о критичности выявленных уязвимостей (в табличном и графическом виде);
      4.1.4. данные об уязвимостях по производителям ПО и оборудования (в графическом виде).
5. Импорт данных об уязвимостях из БД NIST NVD.
   5.1. Система должна автоматически проверять наличие обновлений данных NIST NVD и получать файл с обновлением.
   5.2. Система должна производить регистрацию вновь обнаруженных и обновление изменившихся уязвимостей из файла-источника обновлений.
   5.3. При импорте данных система должна автоматически пополнять справочники производителей, ПО, оборудования, версий в случае отсутствия в БД системы необходимых данных о регистрируемой уязвимости.

Основываясь на анализе предметной области, была составлена контекстная диаграмма процесса «как будет».

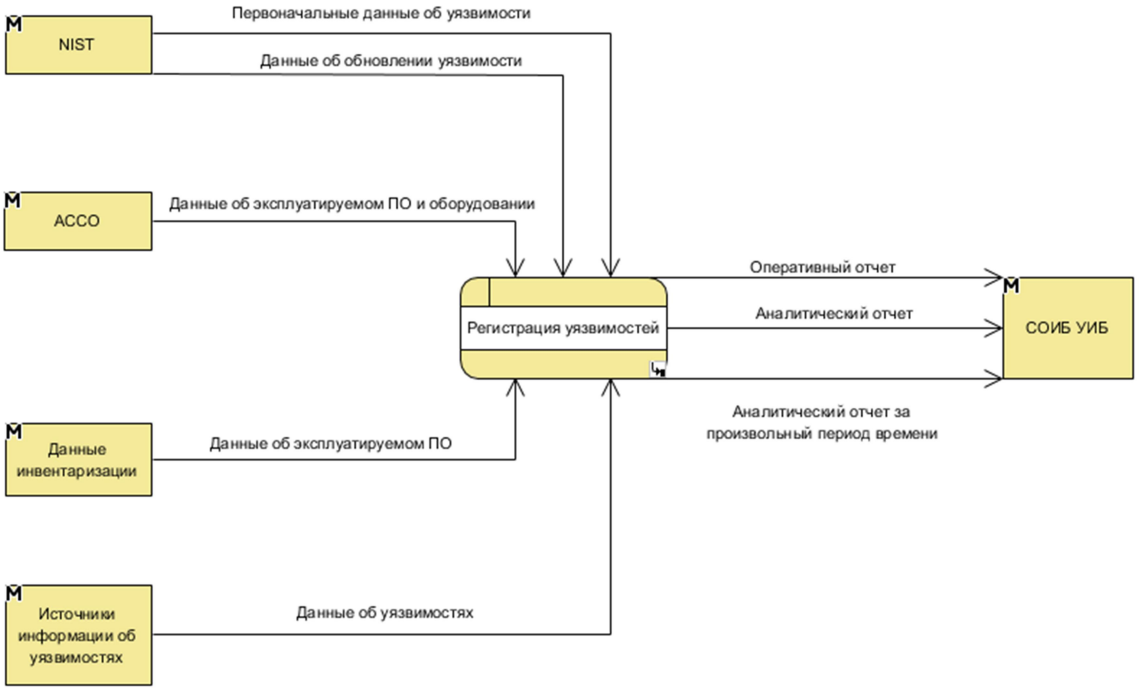

Рисунок 3 – Контекстная диаграмма процесса «как будет»

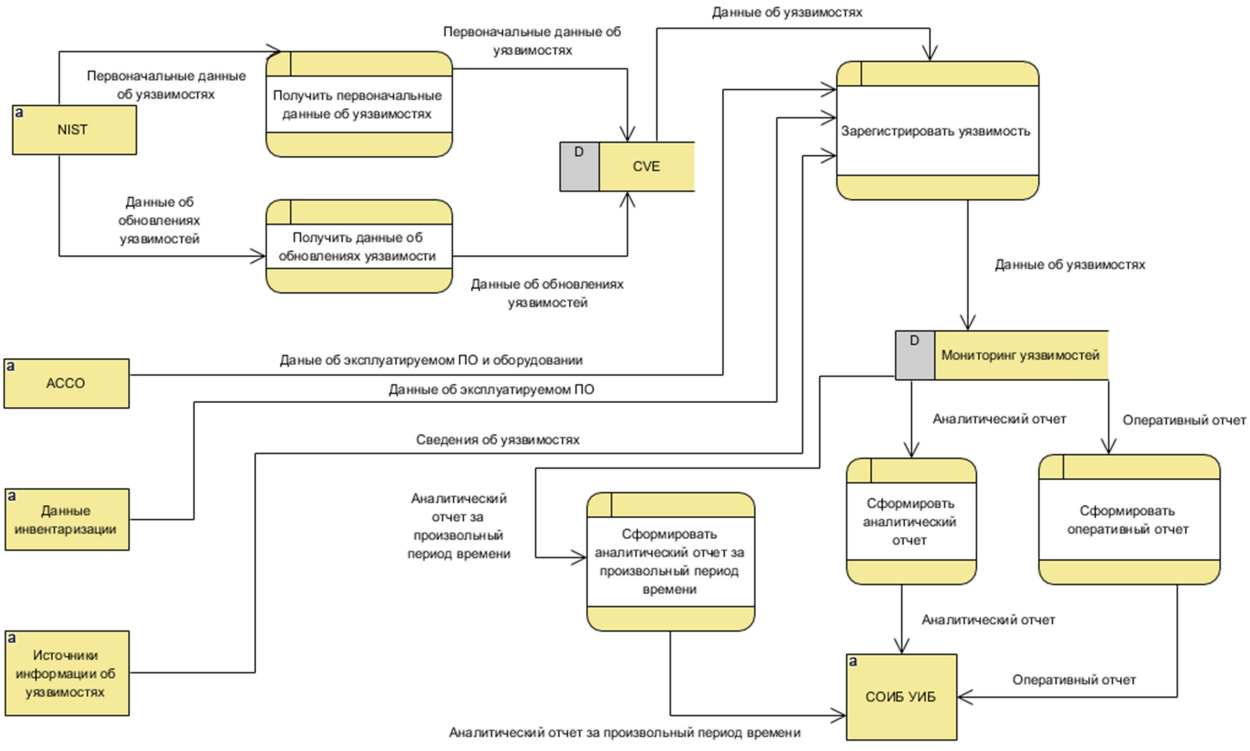

Рисунок 4 – Декомпозиция процесса

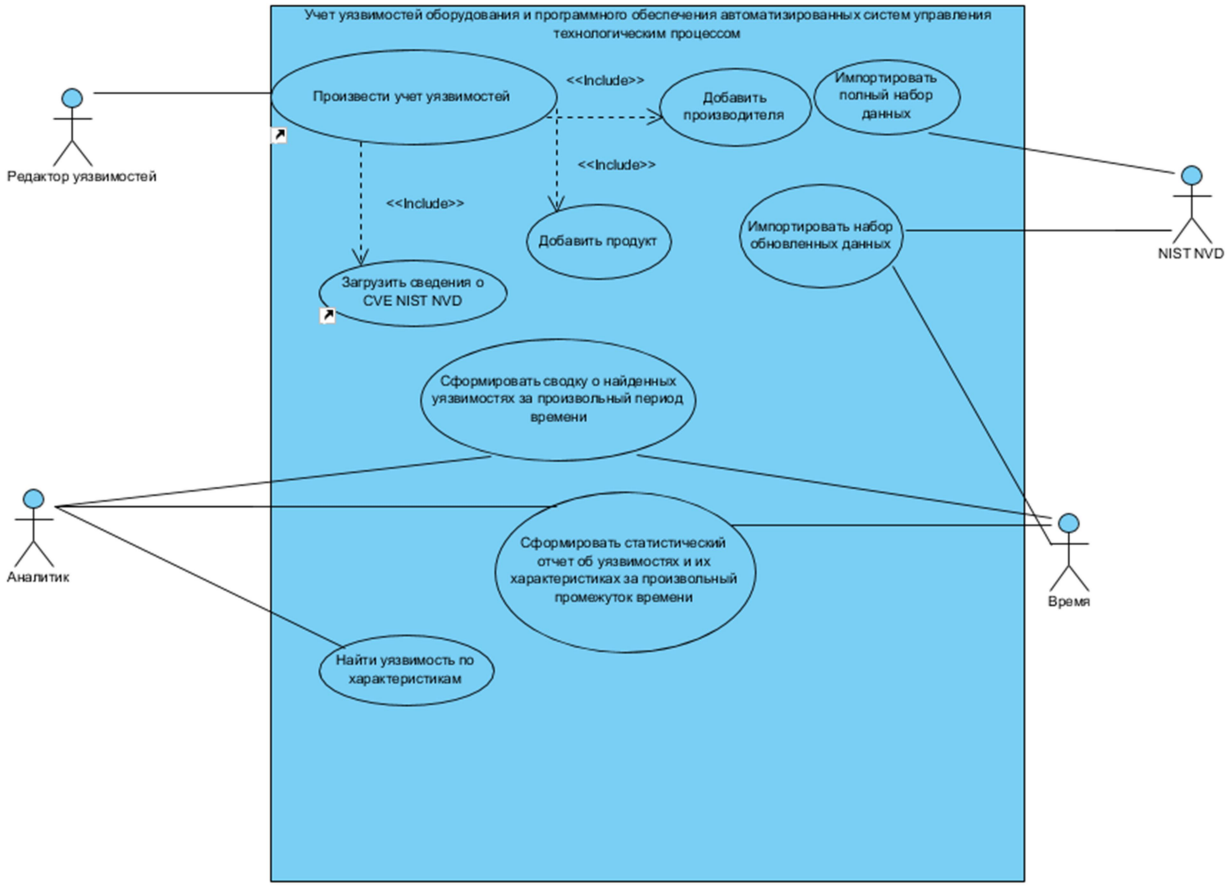

Рисунок 5 – Use Case диаграмма

Представленная выше диаграмма прецедентов, полностью демонстрирует взаимодействие пользователей системы с системой. На диаграмме представлены следующие актеры:

1. Редактор уязвимости – заносит данные об уязвимости, ПО, которое используется на предприятии, в единую базу данных предприятия.
2. Аналитик – формирует формы отчетов, и сами отчеты об уязвимостях, а также делает выборки из уязвимостей.
3. NIST NVD – база данных NIST, где публикуются JSON-файлы с данными об уязвимости.
4. Время – показатель протекания процессов, мера длительности.

Результат разработки

Сама система представлена на диаграмме развертывания ниже:

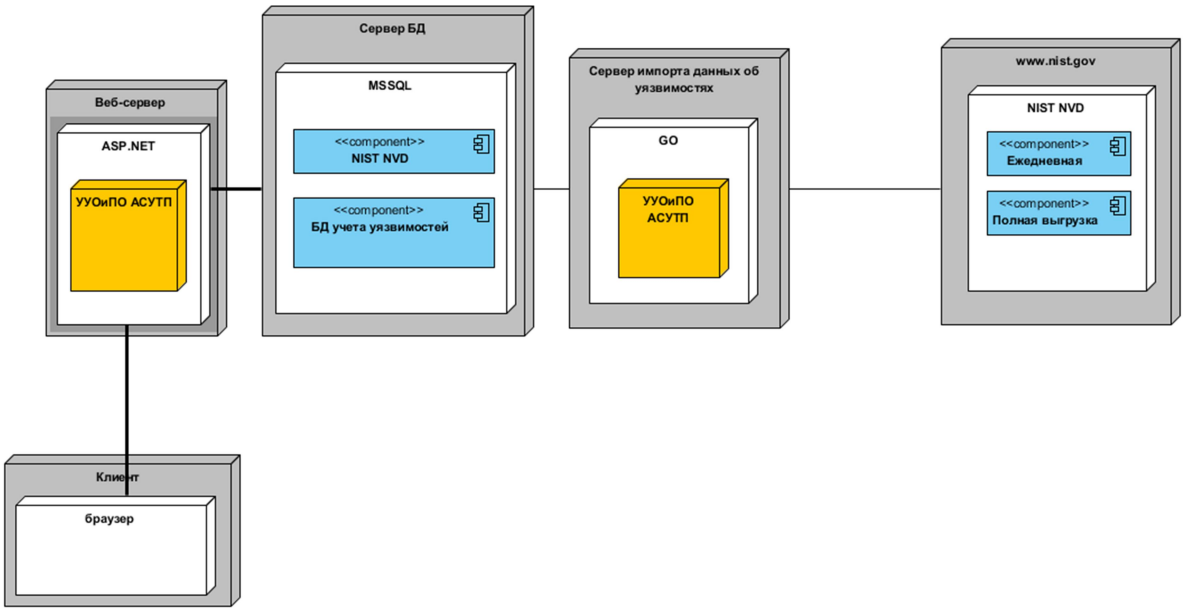

Рисунок 61 – Диаграмма развертывания

На данной диаграмме присутствуют следующие элементы:

1. БД NIST NVD
2. GO.
3. СУБД
4. Веб – сервер
5. Клиент

1. База данный NIST NVD.

База данных NIST NVD содержит в себе файлы формата JSON, в которых структурированно хранится информация об уязвимостях.

Данные об уязвимости и её оценки публикуются на сайте NIST в виде прикреплённых файлов формата JSON.

JSON (JavaScript Object Notation) – текстовый формат обмена данными, основанный на JavaScript. Как и многие другие текстовые форматы, JSON легко читается людьми. Формат JSON был разработан Дугласом Крокфордом. (https://ru.wikipedia.org/w/index.php?search=json&title=Служебная %3AПоиск&go=Перейти)

2. GO.

Для скачивания JSON файлов с базы данных NIST NVD и заполнения БД нашей системы, используется следующий алгоритм:

1. получаем файл по ссылке из сети интернет;
2. распаковываем файл (разархивация);
3. импортируем json в сеть объектов;
4. сохраняем объектную сеть в БД системы.

Реализован данный алгоритм был при помощи языка GO (GOLang).

Golang, или Go – язык программирования, начало которого было положено в 2007 году сотрудниками компании Google: Робертом Гризмером, Робом Пайком и Кеном Томпсоном. (https://ru.wikipedia.org/wiki/Go)

3. Средство управления базами данных.

При разработке как СУБД использовалось Microsoft SQL Server.

Microsoft SQL Server – система управления реляционными базами данных (РСУБД), разработанная корпорацией Microsoft. Основной используемый язык запросов – Transact-SQL.

Средой управления для сервера была выбрана MS SQL Management Studio 17.

SQL Server Management Studio (SSMS) – это интегрированная среда для доступа, настройки, администрирования и разработки всех компонентовSQL Server, а также управления ими. Среда SSMS сочетает в себе обширный набор графических инструментов с рядом отличных редакторов скриптов, обеспечивая разработчикам и администраторам любой квалификации доступ к SQL Server.
(https://ru.wikipedia.org/w/index.php?search=SQL+Server+Management+Studio+&title=Служебная %3AПоиск&go=Перейти)

4. Веб – сервер

В качестве платформы для разработки веб – приложения использовался ASP.NET.

ASP.NET (Active Server Pages для .NET) – платформа разработки веб-приложений, в состав которой входит: веб-сервисы, программная инфраструктура, модель программирования, от компании Майкрософт. ASP.NET входит в состав платформы .NET Framework и является развитием более старой технологии Microsoft ASP.

Сама структура веб – приложения будет построена при помощи шаблона MVC (Model-View-Controller). Следовательно мы будем использовать ASP.NET MVC. (https://ru.wikipedia.org/wiki/ASP.NET)

Заключение

На данный момент реализовано Веб – приложение системы, значительно ускоряющая и облегчающая процесс мониторинга уязвимостей на предприятии, а также последующей регистрации и выпуска отчетностей. Без системы, сотрудник тратит большое количество времени на поиск и добавление информации по уязвимостям. При автоматизации процесса данная операция выполняется значительно быстрее, данные ведутся более структурированно, появилось возможность выпуска различных отчетов за промежутки времени.

Список литературы

1. Общая характеристика уязвимостей информационной системы [Электронный ресурс] // Life-prog. URL: https://life-prog.ru/1_1126_obshchaya-harakteristika %20uyazvimostey-informatsionnoy-sistemi.html. (дата обращения: 18.05.19).

2. Статья об оценке уязвимостей [Электронный ресурс]. URL: https://habr.com/ru/company/pt/blog/266485/ (дата обращения 12.01.2019).
3. Статья про NIST [Электронный ресурс]. URL: https://www.securitylab.ru/news/tags/NIST/ (дата обращения 18.01.2019).
4. Список уязвимостей на сайте NIST [Электронный ресурс]. URL: https://nvd.nist.gov/vuln/full-listing (дата обращения 05.02.2019).

List of references

1. General characteristics of information system vulnerabilities, Life-prog, https://life-prog.ru/1_1126_obshchaya-harakteristika %20uyazvimostey-informatsionnoy-sistemi.html, accessed May 18, 2019.
2. Vulnerability Assessment Article, https://habr.com/ru/company/pt/blog/266485/, accessed Jan 12, 2019.
3. NIST article, https://www.securitylab.ru/news/tags/NIST/, accessed Jan 18, 2019.
4. List of vulnerabilities on the NIST website, https://nvd.nist.gov/vuln/full-listing, accessed Feb 05, 2019.