ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

***«*САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»**

|  |
| --- |
| **Высшая школа кибербезопасности и защиты информации** |
| (наименование учебного подразделения) |

**Отчет о прохождении производственной (преддипломной) практики**

*(вид и тип практики)*

|  |
| --- |
| Орел Евгений Михайлович |

*(Ф.И.О. обучающегося)*

|  |
| --- |
| 6 курс, 3651001/40201 |

*(номер курса обучения и учебной группы)*

|  |
| --- |
| 10.05.01 Компьютерная безопасность |

*(Направление подготовки (код и наименование)*

|  |
| --- |
| **Место прохождения практики:** СПбПУ, ИПММ, Высшая школа кибербезопасности и защиты информации |

*(указывается наименование профильной организации или наименование структурного подразделения*

|  |
| --- |
| г. Санкт-Петербург, Политехническая ул., д. 29 |

*ФГАОУ ВО «СПбПУ», фактический адрес)*

|  |
| --- |
| **Сроки практики:** 02.09.2019 – 23.12.2019 |

|  |
| --- |
| **Руководитель практики от ФГАОУ ВО «СПбПУ»:** |

|  |
| --- |
| Иванов Д.В., к.т.н., доцент |

*(Ф.И.О., уч.степень, должность)*

|  |
| --- |
| **Оценка:** |

|  |
| --- |
| Руководитель практики  от ФГАОУ ВО «СПбПУ»: Д.В. Иванов |

|  |
| --- |
| Обучающийся: Е.М. Орел |

|  |
| --- |
| Дата: 23.12.19 |

СОДЕРЖАНИЕ

[Введение 3](#_Toc29292193)

[1. Анализ основных угроз информационной безопасности сетевой инфраструктуры организации 6](#_Toc29292194)

[1.1. Уязвимости сетевой инфраструктуры 7](#_Toc29292195)

[1.1.1 Стандарт CVSS 8](#_Toc29292196)

[1.1.2 Базы уязвимостей 14](#_Toc29292197)

[1.1.3 Уязвимости, способствующие удаленной компрометации узла 22](#_Toc29292198)

[1.2. Эксплойты 23](#_Toc29292199)

[1.3. Тестирование на проникновение 25](#_Toc29292200)

[1.3.1 Сбор информации 28](#_Toc29292201)

[1.3.2 Проникновение на целевой узел 29](#_Toc29292202)

[1.4. Выводы 30](#_Toc29292203)

[2. Оценка защищенности и выбор мер защиты сетевой инфраструктуры организации 32](#_Toc29292204)

[2.1. Методики оценки защищенности компьютерной сети 32](#_Toc29292207)

[2.1.1 Качественные методики оценки защищенности 32](#_Toc29292208)

[2.1.2 Количественные методики оценки защищенности 36](#_Toc29292212)

[2.1.3 Смешанные методики оценки защищенности 39](#_Toc29292213)

[2.2 Концепция графов атак 43](#_Toc29292214)

[2.3 Показатели защищенности 45](#_Toc29292215)

[2.3.1 Базовые показатели 46](#_Toc29292219)

[2.3.2 Базовые показатели на основе графов атак 47](#_Toc29292220)

[2.4 Методики выбора защитных мер на основе графов атак 49](#_Toc29292221)

[2.4.1 Методика поддержки принятия решений, интегрированная в IDS 49](#_Toc29292222)

[2.4.2 Методики на основе теории игр 50](#_Toc29292223)

[2.4.3 Методики на основе количества достижимых узлов 51](#_Toc29292224)

[2.4.4 Методика на основе показателя процента компрометации сети (NCP) 51](#_Toc29292225)

[2.5 Интегральные показатели 52](#_Toc29292226)

[2.6 Выводы 53](#_Toc29292227)

[3. Разработка методик оценки защищенности и выбора защитных 55](#_Toc29292228)

[3.1 Показатели защищенности узлов сетевой инфраструктуры 55](#_Toc29292229)

[3.2 Методика оценки защищенности сетевой инфраструктуры 58](#_Toc29292230)

[3.3 Методика выбора защитных мер 59](#_Toc29292231)

[4 Реализация системы оценки защищенности и выбора защитных мер 65](#_Toc29292232)

[4.1 Архитектура системы оценки защищенности и выбора защитных мер 65](#_Toc29292233)

[Заключение 70](#_Toc29292234)

[Список использованных источников 72](#_Toc29292235)

[Приложение А 76](#_Toc29292236)

Введение

Внутренняя сетевая инфраструктура практически любой организации представляет собой сложную структуру, состоящую из множества различных сервисов, направленных на поддержание функционирования компании. Эта структура очень динамична: добавляются новые сервисы, меняются конфигурации существующих, создаются новые связи между сервисами. В процессе роста системы процесс обеспечения её информационной безопасности и защита критически важных объектов становятся нетривиальной задачей.

Причиной нарушения информационной безопасности чаще всего становятся:

* уязвимости в операционных системах;
* уязвимости приложений, осуществляющих сетевое взаимодействие с пользователем или друг с другом;
* неправильная конфигурация программного обеспечения;
* ошибки контроля доступа

Используя имеющиеся уязвимости и недостатки системы, внешние и внутренние нарушители проводят сетевые атаки, приводящие к компрометации различных узлов и реализации различных угроз информационной безопасности сети.

Для выявления недостатков компонентов системы, а также поиска уязвимостей и потенциальных векторов атак на информационные ресурсы, проводится анализ защищенности сети. Одним из наиболее эффективных методов анализа является тестирование на проникновение, в ходе которого осуществляется моделирование атак реальных злоумышленников. Такой подход позволяет в полной мере провести оценку защищенности сетевой инфраструктуры, оценить существующие и предложить новые способы защиты.

При этом все возрастающая сложность компьютерных систем: количество узлов в сети, множество различных версий сервисов и потенциальных уязвимостей и наличие средств защиты обуславливает необходимость в разработке автоматизированных систем анализа защищенности сети. Такие системы должны не только проводить анализ сети на наличие уязвимостей, построение трасс атак и их реализацию, но также предлагать оптимальные пути их исправления.

В больших компаниях существует практика устранения только тех уязвимостей, что приводят к проникновению в сеть и компрометации наиболее критических узлов. Из-за сложности сетевой инфраструктуры часто закрывают глаза на остальные цепочки уязвимостей, которые все ещё остаются в локальной сети организации после проведения анализа защищенности, что приводит к повторной компрометации узлов цепочки при нахождении новой точки входа.

Необходимо не только защитить сеть от проникновения извне, но и обеспечить должный уровень защищенности внутренней сети. Так, по данным Positive Technologies за 2019 год [1] при проведении внешнего тестирования на проникновение экспертам удалось преодолеть сетевой периметр 92% организаций, тогда как от лица внутреннего нарушителя был получен полный контроль над инфраструктурой во всех исследуемых системах.

Для оценки уровня защищенности системы в данной работе предлагается использовать подход, основанный на анализе графа потенциальных атак с составлением метрик защищенности узлов и сети в целом для определения наиболее эффективных защитных мер.

Цель данной работы – разработать автоматизированное средство оценки уровня защищенности сетевой инфраструктуры и выбора защитных мер.

Для достижения поставленной цели определены следующие задачи:

* Определить основные классы уязвимостей, приводящие к компрометации узлов, и методы их поиска;
* Проанализировать применимость графов атак в задачах оценки защищенности сети и существующие методики оценки защищенности сети;
* Разработать методику поиска оптимальных защитных мер на основе анализа графа атак;
* Реализовать автоматизированную систему построения графа атак и анализа защищенности сети;

# Анализ основных угроз информационной безопасности сетевой инфраструктуры организации

Сетевая инфраструктура представляет собой совокупность различного оборудования, а также программного обеспечения, которая формирует особую среду для эффективного процесса обмена данными, а также для работы бизнес-приложений. Любая составляющая сетевой инфраструктуры может стать причиной компрометации безопасности сети посредством проведения сетевой атаки или цепочки атак.

Под сетевой атакой принято понимать любой процесс, нацеленный на компрометацию безопасности сети. Результатом выполнения сетевой атаки может стать: захват контроля над удаленной/локальной вычислительной системой, либо её дестабилизация, повышение прав в системе, получение данных пользователей, пользующихся данной вычислительной системой.

Видов сетевых атак огромное множество и часть из них в состоянии реализовать человек, не владеющий большим запасом знаний в области информационной безопасности (далее ИБ). На рисунке 1.1 представлена статистика по различным сетевым атакам за декабрь 2019 года (рисунок 1.1) [https://cybermap.kaspersky.com/stats].

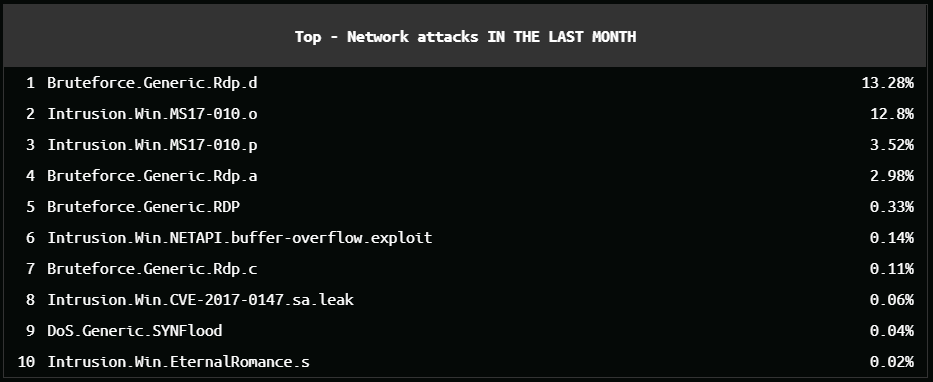


Рисунок 1.1 – Статистика по проведенным сетевым атакам за последний месяц, собранная в Лаборатории Касперского

Наиболее часто встречаются атаки типа подбора пароля к сервису удаленного рабочего стола, а также атаки на SMB-сервер, использующие эксплойты, которые применялись при проведении атак типа WannaCry и ExPetr.

Для осуществления подобных атак необходимо наличие уязвимостей, эксплуатация которых в свою очередь позволит атакующему получить полный доступ к устройству жертвы от ее имени.

## Уязвимости сетевой инфраструктуры

В области информационной безопасности уязвимостью считается любой недостаток системы, используя который злоумышленник может провести атаку на систему. Уязвимость может быть результатом ошибок, допущенных на этапе программирования или проектирования отдельной программы, протокола или запроса, слабых паролей или ненадежных политик доступа.

Наиболее частой причиной возникновения уязвимостей становятся:

* ошибки проектирования, разработки программного продукта, протокола или запроса;
* слабые пароли;
* намеренно оставленные лазейки;
* неправильные настройки оборудования;
* отсутствие надежных политик доступа;
* несанкционированные неумышленные действия пользователей;

В наиболее широком смысле уязвимости можно разделить на две группы: известные и 0-day уязвимости, так называемые «уязвимости нулевого дня». Известные уязвимости хорошо задокументированы исследователями, а соответствующие программные продукты имеют патчи, устраняющие возможность эксплуатации данных уязвимостей. Термин 0-day обозначает не устраненные уязвимости, против которых ещё не разработаны защитные механизмы.

Под угрозой [https://bdu.fstec.ru/ubi/terms] в ИБ понимается любая потенциальная возможность тем или иным образом нарушить информационную безопасность. Попытка реализации такой угрозы посредством уязвимости называется атакой.

В начале 90-х годов стало очевидно, что для хранения всего объема записей о найденных уязвимостях необходимо провести их классификацию и систематизацию. Актуальность данной задачи обуславливалась появлением большого числа нового программного обеспечения: операционных систем, программ, платформ разработки; увеличением количества версий программных продуктов, а также частотой нахождения уязвимостей.

Каждой обнаруженной уязвимости требовалось присвоить некий идентификатор и дать ей краткое описание. Также важно было определить критичность данной уязвимости, например, по таким критериям как простота эксплуатации и последствия эксплуатации. Данная информации впоследствии могла быть дополнена рекомендациями по устранению уязвимости, а также информацией об уязвимых версиях продукта.

В настоящее время для обозначения критичности уязвимости чаще всего используется стандарт Common Vulnerability Scoring System (CVSS).

Разработанные системы накопления знаний об уязвимостях широко используются специалистами по информационной безопасности для оценки защищенности информационных систем, а также нарушителями, осуществляющими попытки их компрометации.

### Стандарт CVSS

Общая система оценки уязвимостей CVSS впервые была опубликована 23 февраля 2005 года исследовательской группой NIAC. Данная система должна была обеспечить универсальность и открытость оценки критичности уязвимостей программного обеспечения, однако, первая версия не была подвержена анализу со стороны организаций, в следствие чего имела ряд недостатков. Основным недостатком CVSS было слишком малое число критериев, по которым проводилась оценка из-за чего существовало множество уязвимостей с одинаковой оценкой. Чтобы избежать подобных недостатков в будущем, была собрана группа CVSS-SIG, задача которой заключалась в выявлении и исправлении всех недостатков CVSS.

Так 1 июня 2007 года было опубликовано описание системы CVSS 2.0, которая в дальнейшем получила широкое распространение. До 2011 года она вошла в следующие стандарты:

* PCI DSS – стандарт безопасности данных платежных карт;
* NIST – национальный институт стандартов и технологий США;
* ITU-T X.1521 – международный стандарт оценки уязвимостей.

CVSS 2.0 оценивает уязвимости по степени серьёзности угрозы и состоит из трех основных групп метрик [https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=51198]: базовой, временной и контекстной, каждая из которых состоит из набора метрик, как показано на рисунке 1.2. При этом каждая метрика представляет собой оценку от 0 до 10 и описание, содержащее информацию для вывода данной оценки.

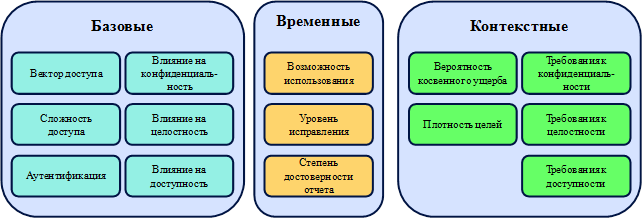


Рисунок 1.2 – Группы метрик CVSS

Группы метрик в стандарте определены следующим образом:

* Базовые метрики представляют внутренние характеристики уязвимости, которые не меняются со временем и средой пользователя.
* Временные метрики представляют характеристики уязвимости, которые меняются со временем, но не от пользовательской среды.
* Контекстные метрики представляют характеристики, которые являются релевантными и уникальными для определенной среды пользователя.

Таким образом, базовые метрики передают основные характеристики уязвимости, что позволяет пользователю получить четкое представление об уязвимости, чтобы затем посчитать временные и экологические метрики, которые более точно отражают критичность уязвимости для их уникальной среды. Данный подход позволяет принимать более обоснованные решения при попытке снизить риски, связанные с уязвимостями.

Для оценки уязвимостей с точки зрения внешнего нарушителя достаточно рассматривать исключительно базовую группу метрик, создающую общее представление об уязвимостях, так как при оценке защищенности системы зачастую отсутствует возможность получения информации о стоимости активов, потенциальном ущербе в результате эксплуатации уязвимости и т.п.

Базовая группа состоит из 6 метрик:

* Способ получения доступа: локальный, удаленный через локальную сеть, удаленный через глобальную сеть. При этом чем дальше нарушитель, тем выше базовая оценка;
* Сложность атаки: низкая, средняя, высокая;
* Показатель аутентификации: не требуется, единственная, множественная. Показатель аутентификации отражает сложность проведения атаки с точки зрения предоставляемых злоумышленником валидных данных;
* Влияние на конфиденциальность: не оказывает, частичное, полное;
* Влияние на целостность: не оказывает, частичное, полное;
* Влияние на доступность: не оказывает, частичное, полное;

Частичным считается влияние на актив, которое может быть ограничено. При наличии физического доступа к системе или прав root, система считается полностью компрометированной.

Данные показатели подставляются в базовое уравнение:

где , и вычисляются следующим образом:

– функция округления до одного десятичного знака после запятой в большую сторону.

В таблице 1.1 сопоставляются качественные и количественные характеристики базовых метрик.

Таблица 1.1 – Шкала оценок базовых метрик

|  |  |  |
| --- | --- | --- |
| **Метрика** | **Качественная характеристика** | **Количественная характеристика** |
| Способ получения доступа | Локальный | 0.395 |
| Удаленный через локальную сеть | 0.646 |
| Удаленный через глобальную сеть | 1.0 |
| Сложность атаки | Высокая | 0.35 |
| Средняя | 0.61 |
| Низкая | 0.71 |
| Показатель аутентификации | Множественная | 0.45 |
| Единственная | 0.56 |
| Не требуется | 0.704 |
| Влияние на конфиденциальность, целостность и доступность | Нет | 0 |
| Частичная | 0.275 |
| Полная | 0.660 |

Однако и в CVSS 2.0 был обнаружен ряд проблем

* Неоднозначная трактовка различных показателей CVSS 2.0 приводила к тому, что в различных базах уязвимостей одни и те же уязвимости имели разную оценку критичности, в виду выбора разных значений метрики сложности эксплуатации;
* Известные компании, такие как Oracle, IBM, Cisco и другие помимо CVSS 2.0 начали использовать оценки собственной разработки, которые являлись более информативными;
* Отсутствие явно определенной области действия ущерба.

В 2015 году была предложена третья версия стандарта, в которой были учтены проблемы второй версии. В неё были внесены следующие изменения:

1. Введен дополнительный уровень доступа: физический;
2. Удален средний уровень сложности эксплуатации уязвимости. В данном стандарте любое дополнительное условие, неподконтрольное нарушителю, приводит к повышению уровня сложности до высокого;
3. Добавлена метрика взаимодействия с пользователем: требуется, не требуется;
4. Метрика аутентификации заменена показатель уровня привилегий, который может принимать значения: отсутствует, низкий, высокий. Первый уровень эквивалентно отсутствию аутентификации, второе – аутентификации от имени обычного пользователя, а третий – аутентификации от имени администратора;
5. Изменены коэффициенты в уравнениях для уменьшения зависимости оценки от сложности эксплуатации и повышения её зависимости от причиняемого ущерба;
6. Определено понятие цепочки уязвимостей. Эксплуатация одной отдельной уязвимости может нести низкую угрозу, однако в цепочке с другими уязвимостями опасность уязвимостей значительно повышается;
7. Метрики воздействия изменены с частичной и полной на низкую и высокую;
8. Добавлена метрика , определяющая область действия ущерба, наносимого уязвимостью. Иногда уязвимости, обнаруженные в одной системе, могут влиять на другие, не связанные с ней, в таком случае предлагается повышать оценку опасности уязвимости. Данный показатель может принимать значения: без изменения, с изменением.

Нововведенная версия CVSS 3.0 позволяет более точно определить опасность уязвимости для системы, однако, и в ней могут быть найдены неоднозначные трактовки, например, при определении влияния уязвимости на целостность, конфиденциальность и доступность информации.

Общая схема оценки уязвимостей по стандарту CVSS представлена на рисунке 1.3

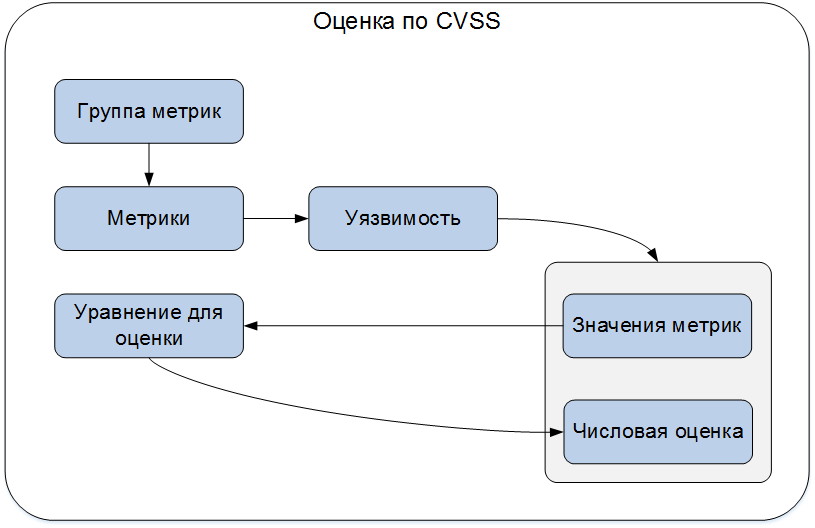


Рисунок 1.3 – Оценка уязвимости по стандарту CVSS

### Базы уязвимостей

Для обнаружения уязвимостей и определения их опасности для исследуемой системы используются базы уязвимостей. Они хранят такую информацию как: идентификатор уязвимости, её краткое описание, подверженные уязвимости версии программного продукта.

На текущий момент существует несколько наиболее распространенных баз уязвимостей[https://cyberleninka.ru/article/n/issledovanie-otkrytyh-baz-uyazvimostey-i-otsenka-vozmozhnosti-ih-primeneniya-v-sistemah-analiza-zaschischennosti-kompyuternyh-setey/viewer]:

1. Банк данных угроз безопасности информации ФСТЭК России [https://bdu.fstec.ru/vul];
2. MITRE CVE [https://cve.mitre.org/about/] и NVD[https://www.kennasecurity.com/blog/using-databases-automate-assessment-remediation/];
3. OSVDB [https://books.google.ru/books?id=9F8oIIPdqiIC&pg=PA161&lpg=PA161&dq=OSVDB+description&source=bl&ots=6UkYYz\_PI2&sig=ACfU3U1gMbWku8-z6Hkv56x3d\_DvIEbclg&hl=ru&sa=X&ved=2ahUKEwjf-vzAouzmAhWG16YKHeZIDkkQ6AEwCXoECAkQAQ#v=onepage&q=OSVDB%20description&f=false];
4. Secunia Advisories and Vulnerability Database [https://www.flexera.com/products/operations/software-vulnerability-research/secunia-research.html];

#### Банк данных угроз безопасности информации ФСТЭК России

На территории Российской Федерации одной из основных организаций, отвечающих за обеспечение информационной безопасности в ключевых системах информационной инфраструктуры, включая компьютерные сети органов государственной власти и компьютерные сети критичных объектов инфраструктуры и предприятий, является Федеральная служба по техническому и экспортному контролю – ФСТЭК России.

Для обеспечения деятельности по сертификации средств защиты информации и обнаружения уязвимостей программного обеспечения, ФСТЭК России с 2014 года поддерживает собственный реестр известных угроз информационной безопасности и уязвимостей программного обеспечения – Банк данных угроз безопасности информации (БДУ ФСТЭК России).

Данный реестр уязвимостей 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. Пополняется реестр ФСТЭК России путем мониторинга общедоступных источников информации – информационных бюллетеней российских и иностранных компаний, производящих ПО, а также реестров и информационных бюллетеней исследовательских организаций и компаний, предоставляющих услуги в области информационной безопасности.

На конец декабря 2019 года данное хранилище содержало порядка 24 тысяч записей об уязвимостях. Все хранящиеся в БДУ ФСТЭК России записи имеют единообразный формат и включают: текстовое описание уязвимости, дату обнаружения уязвимости, названия, версии и производителей уязвимого ПО, информацию о типе ошибки, классе уязвимости и текущем ее статусе (потенциально возможная либо подтвержденная производителями ПО или независимыми исследователями уязвимость, устранена ли уязвимость в новых версиях ПО). Также записи содержат оценку критичности уязвимости и сопутствующий вектор CVSS, пометку о наличии известных готовых сценариев эксплуатации уязвимости и возможного результата эксплуатации уязвимости, указание уязвимых аппаратных платформ или операционных систем, список возможных методов противодействия уязвимости и ссылки на источники дополнительной информации по уязвимости (включая идентификаторы данной уязвимости в иных реестрах и базах данных).

Следует отметить, что записи в базе данных БДУ ФСТЭК России предоставляют более подробную информацию о различных аспектах, связанных с уязвимостью, чем иностранные реестры уязвимостей CVE List и NVD, предоставляемые американскими некоммерческими и государственными организациями.

К возможным недостаткам БДУ ФСТЭК России можно отнести меньшее общее количество покрытых реестром уязвимостей (в сравнении как с базами CVE List и NVD, так и с базами данных уязвимостей, созданных коммерческими компаниями), а также отсутствие какой-либо агрегации отдельных записей (которая характерна для такой базы данных, как Vulnerability Notes Database).

#### MITRE CVE и NVD

Стандарт Common Vulnerabilities and Exposures (CVE), разработанный американской некоммерческой исследовательской корпорацией MITRE Corporation в 1999 году, является на сегодняшний день основным стандартом в области унифицированного именования и регистрации обнаруженных уязвимостей программного обеспечения. Данный стандарт непосредственно определяет, как формат идентификаторов и содержимого записей об отдельных обнаруженных уязвимостях, так и процесс резервирования идентификаторов для новых обнаруженных уязвимостей и пополнения соответствующих баз данных.

В настоящее время (по данным на март 2018 года) поддержкой и администрированием реестра уязвимостей CVE занимается группа из 84 организаций по всему миру, в число которых входят ведущие производители программного обеспечения, телекоммуникационного оборудования и интернет-сервисов, такие как Apple, Cisco, Facebook, Google, IBM, Intel, Microsoft, Oracle и ряд компаний, специализирующихся в области информационной безопасности, например, F5 Networks, McAfee, Symantec, «Лаборатория Касперского» и прочие.

В рамках поддержки проекта MITRE CVE основными задачами этих организаций, называемых CVE Numbering Authorities (CNAs), являются:

* поиск и сбор информации об уязвимостях программного обеспечения (в случае разработчиков и распространителей ПО, их область ответственности ограничена непосредственно их собственными продуктами и сервисами);
* классификация найденных уязвимостей;
* резервирование CVE-идентификаторов для найденных уязвимостей;
* актуализация соответствующей информации в двух официальных каталогах – реестре уязвимостей CVE List самой MITRE Corporation и базе данных уязвимостей NVD (National Vulnerability Database, https://nvd.nist.gov/), поддерживаемой национальным Институтом Технологий и Стандартов США.

На конец 2019 года базы данных Mitre CVE и NVD содержат порядка 125 тысяч записей об отдельных уязвимостях, обнаруженных за период 1999 – 2019 г.

При этом, хотя сами базы данных различаются на уровне функциональных возможностей, предоставляемых пользователям, сами списки записей об уязвимостях фактически идентичны друг другу. Формально CVE List выступает изначальным источником записей для базы данных NVD, а специалисты, отвечающие за поддержку базы NVD, производят уточненный анализ и сбор доступной информации по уязвимостям, зарегистрированным в CVE List (например, собирают ссылки на сторонние источники информации об уязвимости и мерах по ее устранению или предотвращению эксплуатации).

Формат идентификаторов CVE представлен на рисунке 1.2. Он состоит из года регистрации уязвимости – первых четырех цифр и последующих 4-6 цифр, описывающих уникальный номер уязвимости в рамках года уязвимости.

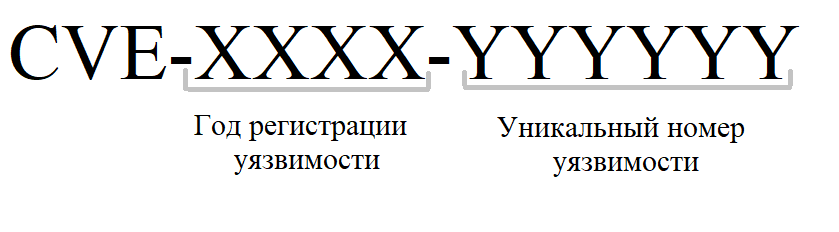


Рисунок 1.2 – Формат идентификатора уязвимостей CVE

Для каждой из обнаруженных уязвимостей запись в базе содержит краткое описание типа и причин уязвимости, уязвимые версии ПО, оценку критичности уязвимости в соответствии со стандартом CVSS и ссылки на внешние источники с информацией об уязвимости – чаще всего, таковыми выступают информационные бюллетени на сайтах производителей программного обеспечения или исследовательских организаций.

В CVE List поддерживаются возможности простейшего поиска среди записей (по ключевым словам и CVE-идентификаторам) и скачивания архивов записей за любой выбранный год в различных форматах (HTML, XML, CVRF, CSV или Plain Text). Также возможно автоматическое получение обновлений в машиночитаемом виде через CVE Data Feed – список изменений, позволяющий отслеживать появление новых идентификаторов CVE, а также изменения в записях уже существующих уязвимостей.

Для базы NVD в свою очередь доступны продвинутые функции поиска уязвимостей по ключевым словам, временным диапазонам создания\модификации записи, компонентам CVSS-метрики и т.п. Кроме того, доступны скачивание всех записей базы данных в XML, а также получение информации об обновлениях базы в виде RSS-подписки и JSON data feed.

Преимуществом баз данных MITRE CVE List и NVD являются ежедневное обновление реестров известных уязвимостей и продолжительность сбора данных (20 лет). При обнаружении новой уязвимости производителем ПО или исследовательской организацией под нее оперативно регистрируется новый идентификатор CVE и создается запись в базе, после чего происходит периодическое обновление информации.

Следует отметить, что в настоящее время среди участников CVE Numbering Authorities лишь две организации имеют статус корневых CNAs, находящихся под непосредственным администрированием Primary CNA (самой MITRE Corporation). На рисунке 1.3 представлена иерархическая структура CNAs.

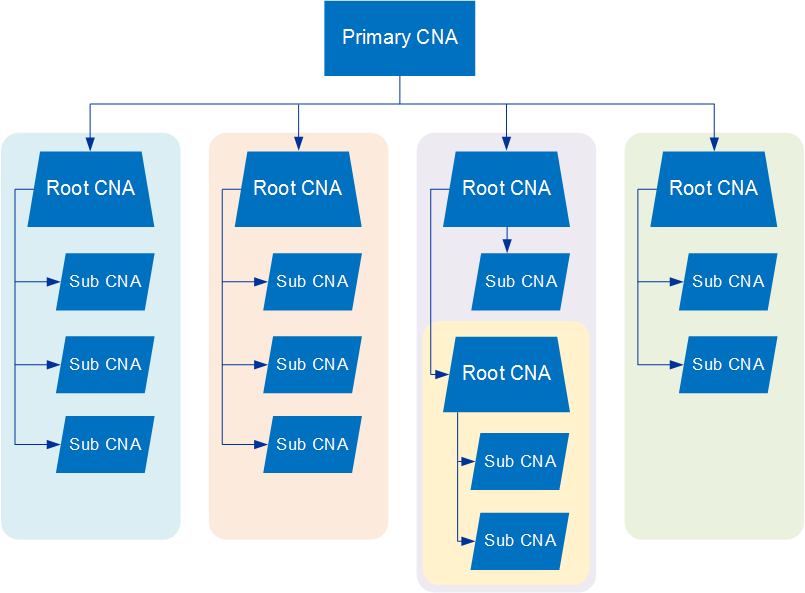


Рисунок 1.3 – Иерархическая структура CNAs

Некоторым естественным ограничением баз данных CVE List и NVD является отсутствие в записях об уязвимостях какой-либо информации о точном месте локализации уязвимости в коде уязвимого ПО и возможных векторах атак, посредством которых возможна эксплуатация данной уязвимости. В некоторых случаях данная информация может быть найдена по ссылкам на внешние ресурсы, однако в большинстве случаев производители и поставщики ПО избегают публикации данной информации, причем не только на период разработки и внедрения патчей, закрывающих обнаруженную уязвимость, но и в последующем.

#### OSVDB

База уязвимостей Open Source Vulnerability Database (OSVDB) была создана в 2004 году по окончанию конференций DEF CON и Blackhat. Для поддержания данной базы знаний в 2005 году была сформирована организация Open Security Foundation, специалисты которой проводили агрегацию данных об уязвимостях из открытых источников, а также собственные исследования программных продуктов для обнаружения новых уязвимостей и сценариев их эксплуатации. Обнаруженные уязвимости проходили классификацию и валидацию, после чего заносились в OSVDB с ссылками на конкретные исследования, списки уязвимого ПО и способы устранения уязвимости.

Однако в 2016 году произошло закрытие базы данных уязвимостей с последующим его перерождением в коммерческий продукт VulnDB. На конец декабря 2019 года данная база содержит порядка 140 тысяч записей об уязвимостях, часть из которых отсутствует в базах CVE List и NVD. Данная база пополняется в среднем 50 записями об уязвимостях каждый день.

#### Secunia Advisories and Vulnerability Database

Secunia Advisories and Vulnerability Database - это база данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО. Бюллетени формируются на основе собственных исследований специалистов Secunia Research и агрегации информации об уязвимостях, полученных из иных публичных источников.

Бюллетени в базе данных Secunia зачастую публикуются еще до того, как соответствующие записи появляются в базе CVE List, и уже впоследствии размечаются ссылками на соответствующие CVE-идентификаторы. При этом нередки ситуации, когда никто из CVE Numbering Authorities так и не берется за регистрацию обнаруженной уязвимости, в результате чего соответствующая запись из базы Secunia Research так и остается без выделенного CVE-идентификатора и, соответственно, не попадает в базы CVE List и NVD.

По своей структуре записи в базе Secunia сходны с содержимым баз CVE List и NVD и содержат дату регистрации уязвимости, тип и краткую классификацию уязвимости, критичность уязвимости (описывается с помощью перечислимого типа Secunia Research Criticality Rating вместо скалярной оценки по стандарту CVSS), списки уязвимого ПО и его версий, ссылки на внешние источники информации и рекомендации по устранению угрозы (как правило, установку патчей от производителя ПО или апгрейд уязвимого ПО до безопасной версии – в этом случае бюллетень содержит упоминание минимального номера безопасной версии).

Характерной особенностью Secunia Advisories является агрегирование в одной записи информации о множестве отдельных уязвимостей, одновременно обнаруженных в одном и том же программном обеспечении. Это означает, что одной записи из базы данных Secunia может соответствовать множество различных CVE-идентификаторов. База данных Scunia Research пополняется с 2003 года.

При бесплатном доступе к данным Secunia информация об уязвимостях предоставляется только в формате html. Для коммерческого использования доступ к базе данных от Secunia Research предоставляется посредством специализированного средства Software Vulnerability Manager и соответствующей подписки на сервис компании Flexera, которой и принадлежит с 2015 года Secunia Research.

### Уязвимости, способствующие удаленной компрометации узла

Компрометация узла возможна в том случае, если злоумышленнику удаётся удаленно выполнить произвольный код на целевом узле. Уязвимости, способствующие проникновению на узел можно поделить на следующие типы [https://xakep.ru/2017/04/10/hacking-attack-types/]:

1. недостатки управления учетными записями и паролями;
2. уязвимости веб-приложений;
3. недостатки фильтрации трафика;
4. недостатки управления уязвимостями и обновлениями;
5. плохая осведомленность пользователей в вопросах информационной безопасности;
6. недостатки конфигурации и разграничения доступа;

Любая уязвимость каждого из этих типов может способствовать проникновению на удаленное устройство. Иногда для проникновения используются комбинации данных уязвимостей, однако это лишь повышает сложность атаки, но не увеличивает вероятность проникновения.

## Эксплойты

Эксплойт [<https://www.gizmosphere.org/network-security-vulnerabilities-vs-exploits/>] – последовательность действий, скрипт или программа, разработанная исключительно для эксплуатации определенной уязвимости. В процессе проведения сетевой атаки могут задействоваться одновременно несколько эксплойтов для достижения поставленных целей. При этом необходимо успешное выполнение каждого из эксплойтов. Закрытие любой из уязвимостей подобной цепочки приведет к несостоятельности исходной атаки.

Эксплойтом может также являться обычный текст или словестное описание того, как проэксплуатировать уязвимость. Чаще всего для написания эксплойтов используются следующие языки программирования: Python, Ruby, PHP, Perl, HTML, Javascript, C/C++.

В общем случае определяют 2 вида эксплойтов:

* удаленный – эксплуатирует уязвимость удаленной системы без предварительного доступа к ней;
* локальный – эксплуатирует уязвимость локальной системы. Требует наличие предварительного доступа к целевой системе. Чаще всего используется для повышения привилегий.

Так как эксплойты разрабатываются для выполнения различных действий на атакуемой системе, то они могут классифицироваться по объекту назначения [<https://www.anti-malware.ru/threats/exploits>]:

* для браузеров и дополнений к ним;
* для операционных систем;
* для офисных программ, проигрывателей и другого прикладного программного обеспечения;
* для серверного программного обеспечения;
* для веб-сервисов, например, WordPress, Joomla, Drupal и др.
* для аппаратных компонентов.

Большинство существующих эксплойтов входят в ту или иную базу эксплойтов. Часть из них находится в открытом доступе, другая – продается в «DarkNet».

Наиболее распространенные базы эксплойтов [<https://null-byte.wonderhowto.com/how-to/top-10-exploit-databases-for-finding-vulnerabilities-0189314/>]:

* 0day.today – база данных эксплойтов, работающая на коммерческой основе. Содержит множество эксплойтов, недоступных в открытых источниках. Доступна только через TOR;
* Rapid7 – база данных, содержащая рекомендации по исправлению уязвимостей, а также ссылки на модули Metasploit Framework, которые автоматизируют эксплуатацию эксплойта;
* Exploit-db – архив общедоступных эксплойтов и уязвимого программного обеспечения, разработанный для использования в процессе тестирования на проникновение.

## Тестирование на проникновение

Тестирование на проникновение – это услуга в сфере информационной безопасности, суть которой заключается в санкционированной попытке проникнуть в информационную систему и обойти существующий комплекс средств ее защиты.

Процесс тестирования на проникновение предусматривает моделирование реальных действий злоумышленника, поиск уязвимостей системы защиты и их дальнейшую эксплуатацию. Тест на проникновение позволяет получить независимую оценку и экспертное заключение о состоянии защищенности сетевой инфраструктуры организации.

Существует несколько подходов к проведению тестирования на проникновение (рисунок 1.4):

Метод белого ящика – подход, при котором тестировщик имеет полный доступ к глубоким знаниям о функционировании и основных атрибутах системы. Это тестирование очень эффективно, так как понимание каждого аспекта системы очень полезно при проведении обширных испытаний на проникновение;

Метод серого ящика – подход, при котором тестировщик получает ограниченную информацию о системе (например, знания алгоритма, архитектуры, внутренних состояний) для имитации внешней атаки на систему;

Метод черного ящика – подход, при котором тестировщику предоставляется только высокоуровневая информация (например, URL или IP-адрес организации) для проведения тестирования на проникновение. Это весьма трудоемкий подход, так как тестировщику требуется значительное количество времени для изучения свойств и деталей системы; кроме того, высока вероятность пропустить часть областей из-за недостатка времени и информации. Также значительно усложняется оценка рисков, ввиду отсутствия знаний о бизнес-логике организации.



Рисунок 1.4 – Подходы к проведению тестирования на проникновение

Именно тестирование методом черного ящика позволяет максимально приблизить процесс тестирования на проникновение к хакерской атаке, от которой организация стремится защитить свои активы.

Разрабатываемые в данной работе методики оценки защищенности и выбора защитных мер способны обеспечить корректную выработку рекомендаций не зависимо от метода тестирования.

Процесс тестирования на проникновение в общем случае состоит из 4 этапов [https://cyberleninka.ru/article/v/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy-bezopasnosti-v-korporativnyh-sistemah]:

1. Планирование;
2. Сбор информации о системе;
3. Проникновение на целевой узел (атака);
4. Составление отчёта.

Этап планирования включает в себя сбор требований, определение сферы применения, стратегий и целей тестирования проникновения в соответствии с нормами безопасности. Кроме того, он может содержать оценку и перечисление проверяемых областей, типы планируемых испытаний и другие связанные с этим проверки.

На втором этапе осуществляется сбор и анализ максимально подробной информации о системных и связанных с ними атрибутах безопасности, которая напрямую влияет на эффективность тестирования системы. Также на данном этапе тестировщики выявляют и обнаруживают уязвимые области системы, которые в дальнейшем будут использоваться для увеличения контроля над системой.

Этап проникновения включает в себя фактическое испытание обнаруженных уязвимостей. Проникновению могут подвергнуться как внешние узлы сетевой инфраструктуры, так и внутренние, расположенные в локальной сети организации.

Этап составления отчётности включает в себя документационную работу по мероприятиям, проводимым на всех упомянутых этапах. Кроме того, она может описывать различные риски, выявленные проблемы, уязвимые области (использованные или нет) и предлагаемые для устранения недостатков решения.

В процессе тестирования возможно возвращение ко второму этапу при обнаружении новых целей. Более того, на каждом этапе может быть задействовано неограниченное число дополнительных операций.

Тестирование на проникновение системы может осуществляться с использованием любого из следующих подходов:

* ручное тестирование;
* автоматическое тестирование;
* сочетание ручного и автоматического тестирования.

Общая схема проведения тестирования выглядит следующим образом (рисунок 1.5).

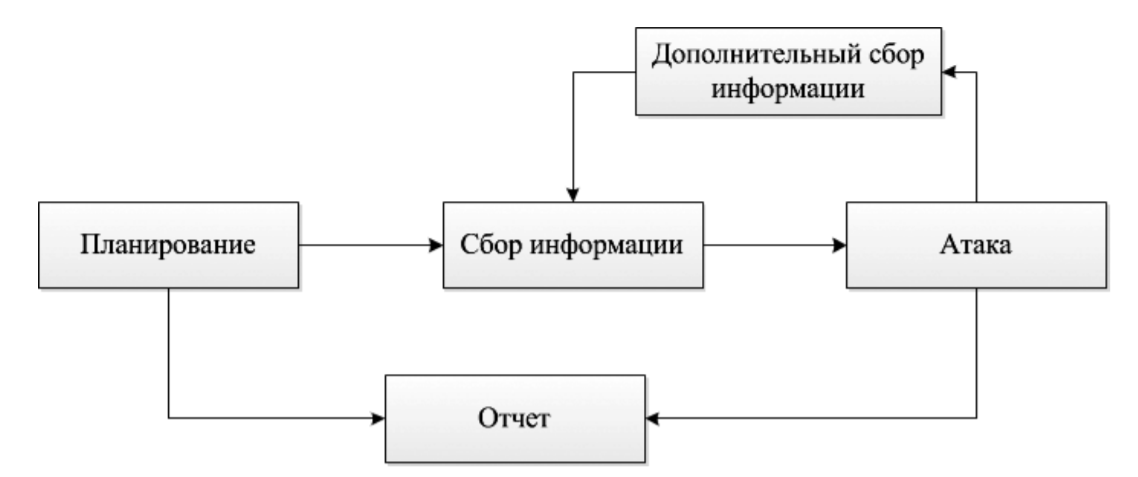


Рисунок 1.5 – Процесс тестирования на проникновение

Оценка защищенности сетевой инфраструктуры проводится на основании информации, полученной на этапе сбора информации о системе и подтвержденной на этапе проникновения. Данные этапы рассматриваются более подробно в п.1.3.1 и п.1.3.2.

### Сбор информации

Разнообразие приложений, протоколов, операционных систем и прошивок оборудования ставит перед тестировщиком задачу по точной идентификации как самого сетевого устройства, так и установленного на нем программного обеспечения и других важных для этапа проникновения параметров.

На этапе сбора информации о системе осуществляется:

* Определение всех доступных узлов системы;
* Определение имен хостов;
* Определение контактной информации сотрудников организации;
* Определение типа узлов;
* Определение типа и версии операционных систем;
* Получение баннеров с обнаруженных портов;
* Определение типа и версий определенных сервисов;
* Определение разделяемых ресурсов;
* Определение пользователей и групп сервисов;
* Идентификация средств защиты;
* Получение списка актуальных уязвимостей;
* Получение списка доступных эксплойтов.

Для осуществления вышеописанных действий могут быть использованы различные автоматизированные сканеры, например, Devsploit, RedHawk, Nmap, Nessus или OpenVAS и снифферы, например, WireShark. Для определения уязвимых версий программного обеспечения, а также доступных эксплойтов могут использоваться базы данных, описанные в п.1.1.2 и п.1.2 данной работы. Определение имен хостов и контактной информации сотрудников может быть осуществлено с помощью сервисов WHOIS или запросов к DNS-серверу.

Помимо автоматического поиска уязвимостей обязательно проводится ручной поиск уязвимостей на основе опыта, накопленного тестировщиком.

На основании полученных данных проводится выявление потенциальных векторов атак и их апробирование.

### Проникновение на целевой узел

На данном этапе осуществляется проверка ранее обнаруженных уязвимостей и недостатков системы путем их эксплуатации. Таким образом, подтверждается или опровергается факт наличия той или иной уязвимости и определяется её влияние на информационную безопасность сетевой инфраструктуры организации.

На этапе проникновения используются как автоматизированные утилиты (Metasploit, Autopwn, Armitage и т.п.), содержащие набор готовых модулей для эксплуатации уязвимостей, так и написанные вручную эксплойты.

В результате проникновения на очередной узел тестировщик может получить: информацию об учетных записях пользователей системы и сервисов (Системы Управления Базами Данных (СУБД), почты, Системы контроля версий, и т.п.); исходные коды различных проектов; доступ к ранее недоступным узлам или новой сети и т.д.

Полученный в результате проникновения доступ к узлам системы и новым сетям используется на этапе сбора информации для расширения покрытия сети тестировщиком.

## Выводы

В данной главе была рассмотрена концепция тестирования на проникновение: понятие уязвимости и эксплойта, крупнейшие базы уязвимостей и эксплойтов, общая система оценки уязвимостей CVSS, основные подходы к тестированию и этапы его проведения.

В процессе тестирования на проникновение рейтинг CVSS может сыграть ключевую роль при определении векторов атак, однако, он не может быть в полной мере использован для оценки защищенности отдельного узла или сетевой инфраструктуры, так как расчет вероятности эксплуатации конкретной уязвимости, эксплойты к которой отсутствуют в открытом доступе, является трудно решаемой задачей. Анализ уязвимости и написание собственного эксплойта может занять намного больше времени, чем выделено на тестирование на проникновение.

Следовательно, в методиках оценки защищенности и выбора защитных мер следует учитывать только те узлы сети и уязвимости, эксплуатация которых привела к компрометации данных узлов.

Информация, полученная на этапе сбора сведений об узлах сети, может быть отфильтрована и использована в качестве метрики критичности компрометации для каждого узла. Такой способ не требует наличия дополнительной информации о системе, предоставить которую может только заказчик, и, как следствие, позволяет быстрее разработать набор рекомендаций по устранению уязвимостей.

Данная метрика будет использована в главе 3 при разработке алгоритмов оценки защищенности сетевой инфраструктуры.

# Оценка защищенности и выбор мер защиты сетевой инфраструктуры организации

Оценка защищенности сетевой инфраструктуры – это устоявшийся метод выявления слабых мест организации. Обеспечить полноценную оценку безопасности информационных систем, содержащих сотни или тысячи узлов, и выбор мер защиты задача нетривиальная. В данной главе рассматриваются основные методики оценки защищенности компьютерных сетей, характеристики систем и узлов, определяющие показатели защищенности, на основании которых проводится поиск оптимальных защитных мер.



## Методики оценки защищенности компьютерной сети

Оценка защищенности компьютерной сети – это процесс выявления уязвимостей, угроз и рисков, связанных с активами организации и мер защиты, которые могут смягчить эти риски [2]. Существует два базовых подхода к оценке защищенности: качественный и количественный, а также смешанный подход, представляющий собой совокупность обоих подходов.

## *Качественные* методики оценки защищенности

Качественные методики позволяют идентифицировать уязвимости и угрозы, описать причины их возникновения, возможные последствия и применяемые защитные меры и на их основе ранжировать риски, однако такие методики не позволяют определить численную величину риска.

Методика оценки риска называется качественной, если в процессе её выполнения формируется качественная оценка уровня риска. И.А. Педерсен и Н.Е. Брюковецкая определили несколько этапов качественной оценки риска (рисунок 1.1) [3]

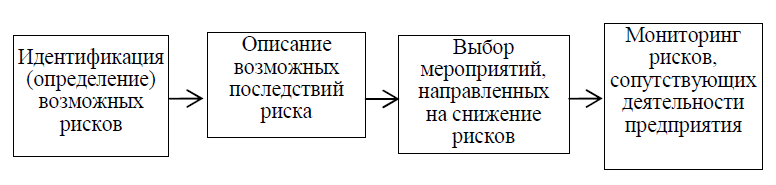


Рисунок 1.1 – Последовательность проведения качественного анализа рисков

Качественные методики используют опыт и суждения экспертов, а не математические формулы. Они также могут использовать опросы для определения уровня угрозы и ожидаемых рисков. Данные методики особенно эффективны, когда невозможно определить денежный эквивалент конкретного риска.

Качественные методики не требуют больших математических вычислений, но результаты, как правило, менее точны, чем полученные при количественной оценке.

Примеры качественных методик:

* COBRA [4];
* OCTAVE [5];
* FRAP [6].



#### Методика COBRA

Методика COBRA разработана компанией Risk Associates [7]. COBRA представляет собой процесс анализа рисков на основе экспертных систем, использующих обширную базу знаний по угрозам, уязвимостям и множеству опросников. Данная методика позволяет оценить соответствие оцениваемой системы стандарту ISO 17799 [8].

COBRA включает в себя 2 модуля: COBRA Policy Compliance Analyst и COBRA Data Protection Consultant. Первый позволяет определить, удовлетворяет ли оцениваемая система стандарту ISO 17799 и получить рекомендации. Второй содержит вопросы, позволяющие идентифицировать активы, угрозы, уязвимости и средства защиты.

Результат работы данной методики – отчёты, содержащие оценки рисков и рекомендации по их уменьшению, базирующиеся на общепринятых практиках.

#### Методика OCTAVE

Данная методика была создана для решения проблем информационной безопасности США. OCTAVE направлена на выявление, оценку и управление рисками информационной безопасности.

Эта методика помогает организации:

* определить наиболее важные для организации активы;
* выявить уязвимости и угрозы для этих активов (автоматизированное или ручное сканирование инфраструктуры);
* определить и оценить потенциальные последствия для организации в случае реализации угроз;
* инициировать действия по постоянному улучшению средств защиты для снижения рисков.

Данная методика основана на применении экспертных знаний.

#### Методика FRAP

Методика оценки рисков FRAP разработана Томасом Пелтиером. В методике обеспечение информационной безопасности предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере информационной безопасности — процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом.

Основные этапы оценки рисков по FRAP:

1. Определение защищаемых активов производится с использованием опросных листов, изучения документации, использования инструментов автоматизированного анализа сетей;
2. Идентификация угроз. При составлении списка угроз могут использоваться разные подходы:

* заранее подготовленные экспертами перечни угроз, из которых выбираются актуальные для данной сети;
* анализ статистики происшествий в данной сети и в подобных ей — оценивается частота их возникновения;
* «мозговой штурм», проводимый сотрудниками компании.

1. Когда список угроз закончен, каждой из них сопоставляют вероятность возникновения. После чего оценивают ущерб, который может быть нанесен данной угрозой. Исходя из полученных значений, оценивается уровень угрозы.

При проведении анализа, как правило, принимают, что на начальном этапе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной сети, что в последствии позволяет показать эффект от внедрения средств защиты информации.

Оценка производится для вероятности возникновения угрозы и ущерба от нее по следующим шкалам:

* Высокая – высокая вероятность того, что угроза реализуется в течение года;
* Средняя – угроза может быть реализована в течение следующего года;
* Низкая – низкая вероятность того, что угроза будет реализована в течение следующего года.

Ущерб активу определяется схожим образом (высокий/средний/низкий).

1. После определения вероятности возникновения ущерба и величины ущерба эксперты определяют средства, позволяющие снизить риски, ориентируясь на наиболее рентабельные. Данные о рисках и возможных защитных мерах документируются и передаются управляющему лицу.
2. Документирование. Результат работы по FRAP – полный набор документации по угрозам и рискам рассматриваемой системы, а также возможные средства минимизации уровней риска угроз.

## Количественные методики оценки защищенности

Количественные методики описывают возможные риски в денежном или частотном эквиваленте. На основе полученных значений и стоимости реализации мер защиты риски сравниваются для принятия оптимальных мер защиты. При количественном анализе рисков выделяют несколько последовательных этапов (рисунок 1.2) [3].

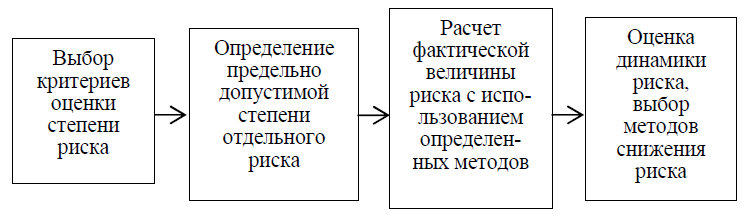


Рисунок 1.2 – Последовательность проведения количественного анализа рисков

К количественным методикам относят:

* RiskWatch;
* ГРИФ.

#### Методика RiskWatch

Методика RiskWatch [9], разработанная при участии NIST, использует значение ожидаемых годовых потерь для оперирования значениями риска (ALE) и значение возврата инвестиций от реализации методов защиты (ROI). На основе данных параметров методика позволяет определить точное соотношение потерь от реализации угроз безопасности и стоимости реализации средств защиты.

В основе методики лежит обширная база знаний, содержащая информацию по активам, угрозам, уязвимостям, видам ущерба, защитным мерам а также опросным листам для оценки факторов риска.

Процесс анализа рисков по методике RiskWatch осуществляется в несколько этапов с использованием одноименного программного обеспечения:

1. Определение параметров исследования. На данном этапе задаются область оценки, категории ущерба, категории активов, рассматриваемые угрозы, уязвимости и применяемые контрмеры.
2. Ввод данных. В ходе данного этапа в систему оценки заносятся данные о ценности активов, вероятности угроз, степени уязвимости, частоте угроз и стоимости контрмер. Ценности активов, определяемой величиной ущерба в результате нарушения конфиденциальности, целостности и доступности активов, соответствуют определенные оценочные денежные величины.

Ожидаемая частота реализации угроз определяется в терминах среднегодовой оценочной частоты угрозы (AFE). База знаний RiskWatch определяет для каждой угрозы стандартную оценочную частоту (SAFE). Для вычисления рисков используется локальная оценочная частота угрозы (LAFE), которая определяется оператором, используя в качестве базового значения SAFE.

Для каждой контрмеры задается её стоимость, которая определяется стоимостью внедрения и сопровождения. Также учитывается, на какой стадии находится реализация контрмеры, продолжительность ее жизненного цикла и насколько эта контрмера уменьшает оценочную частоту реализации угрозы (LAFE).

На данном этапе также осуществляется формирование опросных листов, используемых для получения информации об активах.

1. Оценка рисков. Для проведения оценки рисков производится связывание между собой данных о ценности активов, частоте угроз и степени уязвимости. В результате производится расчет ALE для каждой комбинации актив-угроза-уязвимость. На данном этапе также производится расчет ROI для контрмер и поиск сценария, при котором будет достигнуто максимальное уменьшение рисков при оптимальной комбинации контрмер.
2. Формирование отчётов. На данном этапе подготавливаются отчёты по проведенному анализу рисков. Генерируемые в процессе формирования отчётов графики иллюстрируют статистическую информацию о распределении уязвимостей информационной системы по областям контроля.

Рекомендуемые контрмеры могут быть отсортированы в порядке убывания значения ROI.

#### Методика ГРИФ

Система ГРИФ была разработана компанией Digital Security[10] в 2005 году, как система анализа и управления информационными рисками. Система ГРИФ может проводить несколько видов анализа: на основе модели информационных потоков, требующей от пользователя информации обо всех критически важных ресурсах, о пользователях, которые имеют к ним доступ и их правах доступа, и на основе модели угроз и уязвимостей. Для наших целей наиболее интересной представляется модель анализа угроз и уязвимостей, которая позволяет определить уязвимость каждого ресурса, содержащего информацию, подлежащую защите, и угрозы, которые могут быть реализованы, используя данные уязвимости. В результате работы данной системы создаётся полная картина того, какие слабые места есть в системе и какой ущерб может быть ей нанесен.

Работа системы на основе модели уязвимостей и угроз выполняется в несколько этапов:

1. Пользователь определяет отделы, активы, угрозы и уязвимости информационной системы. Система ГРИФ содержит большую базу знаний об угрозах и уязвимостях, полнота которой достигается благодаря специально разработанной классификации угроз DSECCT, воплотившей в себе многолетний опыт в области ИБ (около 200 уязвимостей и 100 угроз);
2. Для вышеописанных ресурсов системы пользователь определяет связи (актив-отдел, уязвимость-угроза, актив-угроза);
3. Система ГРИФ анализирует полученные данные и генерирует отчёт, содержащий значение риска для каждого актива;
4. На основе полученных отчётов производится поиск оптимальных контрмер для снижения уровня остаточного риска;
5. На выходе система генерирует отчёт об уровне риска каждого актива, результат анализа причин наличия рисков и оценку эффективности различных мер защиты.

## Смешанные методики оценки защищенности

На практике обособленное применение количественных или качественных методик. Смешанные методики сопоставляют качественному уровню определенный количественный диапазон [11].

К таким методикам относятся:

* CRAMM;
* Методики оценки рисков на основе графов атак.

#### Методика CRAMM

Методика CRAMM [12] объединяет в себе количественные и качественные методы для проведения комплексной оценки рисков. Разработана Central Computer and Telecommunications Agency (CCTA) в Великобритании. Данная методика включает в себя следующие этапы:

* Выявление и оценка активов. В качестве активов могут выступать: программное обеспечение, аппаратные ресурсы, либо данные;
* Выявление угроз и уязвимостей;
* Оценка рисков;
* Выбор защитных мер и их приоритизация.

Для оценки потенциального ущерба используется шкала от 1 до 10. Выявление угроз и уязвимостей осуществляется на основе экспертных знаний с помощью опросов. Значение уровня уязвимостей определяется как: высокий, средний и низкий, уровень угроз: очень высокий, высокий, средний, низкий и очень низкий. Риск оценивается в зависимости от годовых потерь по шкале от 1 до 7. Потери зависят от стоимости активов, уровня угрозы и уязвимости. Полученные уровни рисков используются для генерации вариантов защитных мер.

Таким образом, CRAMM комплексно охватывает все этапы управления рисками, начиная от фактического анализа рисков и заканчивая предложением контрмер, включая генерацию выходных данных для документации по безопасности (планирование действий в чрезвычайных ситуациях и обеспечение непрерывности). CRAMM одновременно поддерживается одноименным приложением, которое помогает в сборе данных, а также в расчете и обработке отчета по управлению рисками.

CRAMM также помогает доказать эффективность затрат на управление рисками, безопасность и планирование действий в чрезвычайных ситуациях. Он содержит обширную библиотеку контрмер безопасности. Также применение методики CRAMM позволяет организациям подготовиться к сертификации в соответствии с ISO 27001.

#### Методика оценки рисков на основе графов атак

В работе [13] была предложена методика оценки рисков на основе построения и анализа графа атак для оценки защищенности сети. Данная методика использует модифицированную формулу расчета CVSS для определения уровня риска. Вместо исходного параметр CVSS SecurityRequirements вводится показатель Criticality, определяющий ценность актива для организации, который вычисляется с учетом финансовой стоимости актива и зависимостей свойств безопасности активов. Значения варьируются от 0 до 100. При этом выделяют следующие диапазоны критичности:

* [0:0,01) – ничтожно малая;
* [0,01:0,1) – малая;
* [0,1:1) – значительная;
* [1:10) – повреждающая;
* [10:100) – серьезная;
* 100 – смертельная.

В таблице 1.1 приведено преобразование шкалы для использования в уравнении CVSS.

Таблица 1.1 – Преобразование шкалы оценок критичности

|  |  |
| --- | --- |
| **Критичность** | **Значение** |
| [0:0,01) | 0 |
| [0,01:0,1) | 0,5 |
| [0,1:1) | 1 |
| [1:10) | 1,2 |
| [10:100) | 1,4 |
| 100 | 1,51 |

Уравнение CVSS:

В раскрытом виде:

где – возможность использования уязвимости,

где – влияние на конфиденциальность, целостность и доступность в результате эксплуатации уязвимости; – требования безопасности, а в данном контексте - критичность актива.

Тогда уравнение принимает вид:

где функция Criticality – критичность актива по нарушению конфиденциальности, целостности и доступности.

Исходя из вышеописанных формул риск может принимать значение от 0 до 10. После определения риска каждой уязвимости актива проводится определение риска программного обеспечения, как максимального риска его уязвимостей. Затем проводится оценка риска актива схожим образом. Уровень риска системы определяется как максимальной оценкой риска всех активов системы, как высокий/средний/низкий в соответствии с CVSS. Данная методика позволяет выделить наиболее незащищенные участки системы.

Данная методика наиболее близка к применению в реальных условиях тестирования защищенности сетевой инфраструктуры, так как оценку уязвимостей по CVSS может провести и сторонний наблюдатель в отличие от методик, использующих опросы и требующих указать критичность активов с точки зрения бизнес-процессов организации. Однако, данная методика не учитывает важность самих узлов, но лишь возможность их компрометации путем эксплуатации наиболее критичных уязвимостей. Так, например, два узла, имеющие одинаковые максимальные по критичности уязвимости получат одинаковое значение риска, однако на одном из них может находиться несколько жизненно важных для работы инфраструктуры сервисов, важность которых никак не будет учтена. Также данная методика не описывает меры, принимаемые для снижения рисков.

Таким образом, необходимо разработать методику оценки защищенности сетевой инфраструктуры, которая соответствует следующим требованиям:

* Активы организации представляют собой сетевые узлы;
* Стороннее лицо, проводящее оценку защищенности сетевой инфраструктуры, должно быть способно провести самостоятельную оценку ценности активов для организации;
* Ценность узлов должна определяться на основании общедоступной информации и определяться целочисленным значением;
* Ценность узла должна зависеть от работающих на нем сервисов;
* Выбор защитных мер должен осуществляться с целью минимизации риска всей инфраструктуры.

## Концепция графов атак

Существует множество работ по применимости графов атак в задаче оценки защищенности сетевой инфраструктуры. Они применяются для анализа того, каким образом может развиваться атака внутри сети организации.

Граф атак можно представить как последовательность всех возможных действий злоумышленника для реализации угроз, так называемых трасс атак. Существует несколько общепринятых типов графов атак [14]:

* + Полный граф атак – узлы такого графа представляют собой состояния, а ребра – уязвимости. Такие графы иллюстрируют каждую возможную трассу атак, которую может реализовать нарушитель. Они имеют сложность , что негативно сказывается на их размере и, следовательно, на скорости вычислений. Часть полного графа атак представлена на рисунке 1.3.

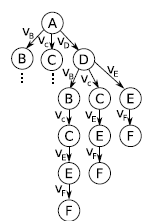


Рисунок 1.3 – Часть полного графа

* + Граф предсказаний – узлы и ребра представляют собой те же сущности, что и в полном графе. Каждый узел попадает в граф предсказаний, если ни один его предок не использует ту же уязвимость для попадания в то же состояние. Данные графы не имеют недостатка полного графа по скорости построения и могут правильно прогнозировать влияние удаления любой из уязвимостей в сети. Как следствие такие графы строятся намного быстрее, чем полные, но тем не менее всё ещё содержат лишние структуры. Пример полного графа приведен на рисунке 1.4.

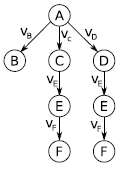


Рисунок 1.4 – Граф предсказаний

* + MP-граф (граф со множеством предусловий) – содержит три типа узлов: уязвимости, состояния и предусловия. Для отображения связей с уже существующими узлами добавляются дополнительные циклические дуги. Данный граф строится быстро и может быть преобразован в полный граф или граф предсказаний. Пример такого графа приведен на рисунке 1.5.

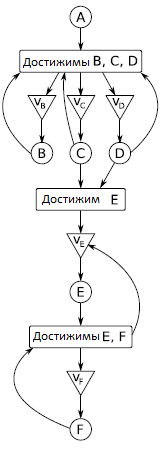


Рисунок 1.5 – MP-граф атак

При работе с графами атак возникает две основные проблемы:

* + Обработка циклов;
  + Значительное время обработки.

Для решения данных проблем применяются различные предположения, такие как: свойство монотонности графа и отказ от повторного посещения узлов; выделяются различные типы циклов графа и производятся расчеты вероятностей применения атакующих действий в зависимости от вида цикла.

## Показатели защищенности

Методики оценки защищенности позволяют определить понятие показателя защищенности – параметра, определяющего качественную или количественную оценку защищенности анализируемой сети.



### Базовые показатели

Базовыми называются показатели защищенности, непосредственно характеризующие элементы конфигурации и безопасности анализируемой системы, такие как: сервисы, установленные на узлах; уязвимости; источники угроз; атакующие действия; защитные меры. Определение их значений не требует проведения дополнительных вычислений.

В частности, в различных работах встречаются следующие виды показателей защищенности:

* В работе [15] показатель защищенности определяется исходя из ущерба сетевой инфраструктуры, связанного с реализацией угроз;
* В работе [16] рассматривается показатель на основе уровня навыков атакующего. Уровень навыков варьируется в зависимости от уровня, атакующего и его знаний о системе, а уровень атакующего определяется на основе максимальной сложности атакующих действий;
* В [17] используется целый ряд показателей защищенности:
  + Суммарное количество обнаруженных уязвимостей;
  + Актив с наибольшим текущим уровнем риска организации;
  + Процент персонала, прошедшего обучение соблюдению политик и процедур информационной безопасности.
* В работе [18] выделяют такие показатели, как стоимость инцидентов, процент активов без уязвимостей, характеризующие количественные и стоимостные характеристики уязвимостей. В качестве показателей конфигурации системы используются метрики количества приложений и сервисов, процент критичных приложений и сервисов и другие.

Рассмотренные показатели защищенности позволяют охватить лишь часть критериев, требуемых для проведения полноценной проверки защищенности. Также большинство рассмотренных показателей требует вмешательства эксперта и дополнительных знаний о системе, что недоступно лицу, проводящему независимую оценку защищенности.

### Базовые показатели на основе графов атак

В работе [19] рассматриваются релевантные исследования в области показателей защищенности, которые делятся на следующие группы:

* Топологические характеристики;
* Стоимостные характеристики;
* Характеристики атаки и реакции на атаку;
* Характеристики системы;
* Характеристики нарушителя;
* Показатели, применяемые при анализе уязвимостей нулевого дня.

Так, в работе [20] выделяются следующие топологические показатели:

* Критичность хоста – зависит от ущерба для бизнеса при потере данного хоста;
* Незащищенность – определяется простотой использования уязвимостей хоста и его достижимостью;
* Нисходящий риск – риск, полученный в результате прохождения через все хосты, атакуемые с данного хоста.

К стоимостным характеристикам относятся такие показатели, как:

* Ожидаемые годовые потери;
* Общий выигрыш – рассчитывается как разница между выигрышем от снижения годовых потерь и затратами на реализацию средств защиты;
* Возврат инвестиций от реагирования на атаку.

В качестве характеристики атаки рассматриваются:

* Потенциал атаки – определяет насколько близко нарушитель находится относительно своей цели;
* Уровень уверенности – определяет меру уверенности в том, что атака осуществляется в текущий момент;
* Показатель уверенности в компрометации – вероятностная величина, определяющая вероятность компрометации определенного узла;
* Ущерб от атаки – показатель, определяющийся на основе ценности активов;
* Эффективность реагирования;
* Выигрыш при реагировании;
* Побочные потери при реагировании.

В качестве характеристики нарушителя рассматривается уровень навыков нарушителя – помогает определить возможность проведения атаки нарушителем.

К характеристикам, используемым при анализе уязвимостей нулевого дня относятся:

* Вероятностная мера уязвимости – определяет насколько вероятно появление уязвимости нулевого дня определенной критичности за определенный срок;
* K-безопасность нулевого дня – определяет устойчивость сети к уязвимостям нулевого дня.

На основании вышеописанных уязвимостей авторы [20] проводят классификацию показателей защищенности, приведенную на рисунке 1.6.

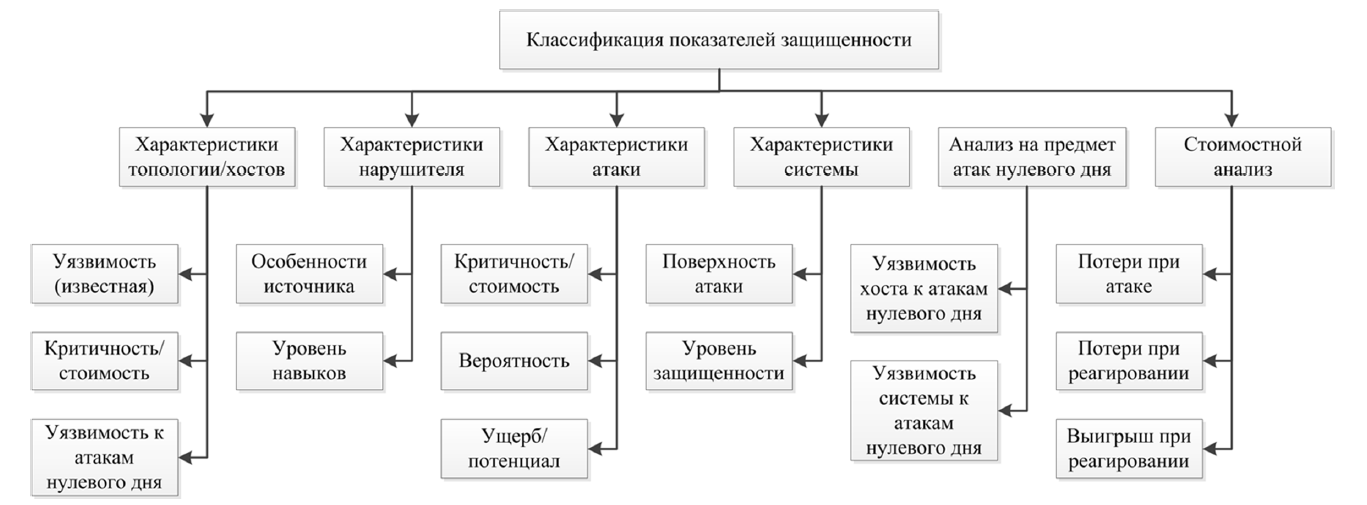


Рисунок 1.6 – Классификация показателей защищенности на основе графа атак

В данной работе за основу предлагается взять подход на основе оценки нисходящего риска, рассчитанного на основе показателя ценности каждого узла для атакующего, достижимого из текущего.

## Методики выбора защитных мер на основе графов атак

В процессе оценки защищенности сетевой инфраструктуры, на этапе выбора защитных мер, необходимо провести приоритизацию и применение соответствующих защитных мер, способствующих понижению уровня риска системы.

Задача поиска оптимальных защитных мер на графе атак является нетривиальной, в виду проблем, описанных в п.1.2.2. В работе [21] описано несколько вариантов решения данной задачи.

### Методика поддержки принятия решений, интегрированная в IDS

Одним из вариантов решения данной задачи является система поддержки принятия решений в выборе контрмер, которая реализуется как часть системы обнаружения вторжений (IDS) [22]. Система содержит хранилище ранее проведенных атак и контрмер, представленных в LAMBDA – универсальном языке, используемом для описания атак в терминах условий, предшествующих эксплуатации (предусловий) и пост-эксплуатации (постусловий).

Контрмеры представлены в LAMBDA следующим образом: предварительное условие представляет собой состояние системы, которое требует применения контрмеры, а постусловие является состоянием системы после применения контрмеры (обычно отрицание предварительного условия). Авторы определили понятия корреляции и антикорреляции следующим образом: два состояния коррелируют, если постусловие одного поддерживает предварительные условия другого (т.е. эти экземпляры представляют собой этапы атаки в сценарии многоступенчатой ​​атаки). Два состояния не коррелируют, если постусловие одного противоречит предварительным условиям второго (т.е. одно состояние представляет собой защитную меру, которая предотвращает появление второго состояния, представляющего атаку). Процесс рекомендаций по противодействию инициируется оповещениями IDS. При получении предупреждения будущие шаги атаки определяются путем поиска корреляций в хранилище, а контрмеры - путем поиска антикорреляций.

Таким образом, для каждого узла графа-состояния строится набор антикорреляций, который не позволит совершить атаку. Метод хорош для противостояния известным атакам в режиме реального времени, но совершенно не подходит при статическом анализе графа с целью минимизации рисков.

### Методики на основе теории игр

Данные методики характеризуются последовательностью состояний и действий атакующего и защитника (стратегии). Изменение состояния происходит при осуществлении действий в рамках определенной стратегии. Защищающая сторона стремится к выбору минимальной по стоимости стратегии, характеризующейся минимизацией затрат и времени, необходимых для реализации всех действий стратегии. На выходе данной методики – оптимальная стратегия, которую администратору необходимо применить для обеспечения защищенности системы.

Преимущество таких методик – учет временного аспекта.

### Методики на основе количества достижимых узлов

В работе [14] рассматривается методика выбора защитных мер на основе показателей, определяющих как много путей атаки будет заблокировано, введением конкретной защитной меры. Защитной мерой в данном случае выступает удаление узла-уязвимости MP-графа. Для упрощения поиска оптимального решения используется дополнительный тип узлов графа, все исходящие ребра которого направлены на узлы-уязвимости, которые требуют одинаковых условий для эксплуатации. Таким образом, остаётся определить, устранение путей к какому из таких узлов принесет наибольшую эффективность. Однако в работе не определяются конкретные показатели защищенности и методы их вычисления.

### Методика на основе показателя процента компрометации сети (NCP)

Данная методика [23] опирается на показатель NCP, определяющий процент узлов, на которых атакующий может получить пользовательский или администраторский доступ. Показатель принимает значения в диапазоне от 0 до 100%. Выбор защитных мер осуществляется следующим образом:

* Производится обход графа в ширину, для каждого узла создаётся список входящих дуг. Дуги соответствуют уязвимостям, которые могут быть применены для компрометации узла;
* Для полученного набора дуг подбираются защитные меры;
* Узлы с одинаковым набором защитных мер объединяются в группы;
* Для каждой защитной меры рассчитывается NCP (каждая защитная мера удаляет одну дугу графа);
* Все защитные меры сортируются по увеличению значения NCP;
* Выбирается мера с наименьшим NCP, то есть такая мера, разница предыдущего и текущего NCP которой максимальна.

Данная методика схожа с методикой, представленной в п.1.2.4.3 данной работы, однако, работает куда медленней ввиду того, что достижимость пересчитывается для каждой отдельной контрмеры.

Большинство рассмотренных методик используют показатели, которые могут быть применены при оценке защищенности системы сторонним лицом, не имеющим доступа к описанию бизнес-процессов организации, реальной стоимости активов и их важности для организации, однако, они не решают проблему сложности графа и устранения циклов.

## Интегральные показатели

Интегральными называются показатели, непосредственно характеризующие безопасность всей сетевую инфраструктуры. Использование интегральных показателей – один из наиболее перспективных путей решения задачи оценки защищенности сети и выбора контрмер [24].

Многие рассмотренные методики на финальной стадии выбора защитных мер используют именно интегральные показатели, потому что они позволяют определить такие характеристики системы как: уровень риска или поверхность атаки, которая определяется на основе ресурсов, которые могут использоваться при проведении атаки. Однако, использование интегральных показателей имеет свои недостатки: перерасчет таких показателей с целью выбора наиболее оптимальных защитных мер занимает значительное время. Уменьшению времени обработки интегральных показателей способствует оптимизация алгоритмов вычисления показателей, либо внедрение ограничений на используемые графы атак.

В данной работе рассматривается методика вычисления интегрального показателя уровня риска с использованием оптимизаций, способствующих уменьшению числа пересчитываемых базовых показателей, на которых базируется показатель уровня риска системы.

## Выводы

В данной главе было рассмотрено множество различных методик оценки защищенности сети, выбора контрмер и показателей защищенности. Наиболее актуальными для данной работы являются методики, основанные на анализе графов потенциальных атак. Такие методики позволяют определить слабые места сетевой инфраструктуры организации и осуществить выбор средств защиты для минимизации рисков.

Методики, основанные на графах атак, допускают ограниченную осведомленность атакующего о топологии сети, её бизнес-процессах и ценности узлов для организации, однако ни одна из рассмотренных методик не может в полной мере обеспечить автоматизацию процесса анализа с полным набором входных данных, доступных для атакующего. При этом не во всех рассмотренных методиках решаются ключевые проблемы использования графов атак в процессе оценки защищенности: наличие циклов и значительное время построения.

Возникает необходимость в создании методики, которая будет соответствовать следующим требованиям:

1. Активы организации представляют собой сетевые узлы;
2. Проверяющий должен быть способен провести оценку защищенности сетевой инфраструктуры, опираясь исключительно на те сведения о системе, которые может получить самостоятельно.
3. Ценность узлов должна вычисляться на основании общедоступной информации и определяться целочисленным значением;
4. Ценность узла должна напрямую зависеть от работающих на нем сервисов;
5. Ценность узла должна зависеть от его типа;
6. В качестве базового показателя защищенности должен быть использован параметр нисходящего риска, вычисление которого основано на ценности достижимых из текущего узла хостов.
7. В качестве интегрального показателя должен выступать уровень риска системы, вычисляющийся как сумма параметров нисходящего риска каждого из узлов графа;
8. Алгоритм выбора защитных мер должен обеспечивать отсутствие циклов и оптимизацию этапа перестройки графа атак;
9. Выбор защитных мер должен осуществляться с целью минимизации уровня риска всей инфраструктуры.

# Разработка методик оценки защищенности и выбора защитных

В данной работе предполагается, что граф атак строится в процессе проведения тестирования защищенности сетевой инфраструктуры (в процессе тестирования на проникновение). В данном случае оценщик имеет сетевой доступ ко всем узлам сетевой инфраструктуры, содержащимся в графе атак.

В качестве основных компонентов оценки защищенности выделим: активы (устройства сети), представленные на графе атак узлами; уязвимости, представленные на графе атак дугами; защитные меры, представляющие собой действие по устранению уязвимости конкретного актива и риск.

Оценка защищенности производится по графу G = (V, A) – ориентированный граф, где V – непустое множество узлов, A – множество триплетов, называемых ребрами, вида , где – идентификатор уязвимости, присутствующей на узле . Направление дуги задаётся последовательностью следования узлов в записи.

## Показатели защищенности узлов сетевой инфраструктуры

В качестве базового показателя защищенности используется значение критичности узла, которое вычисляется на основе информации о запущенных на узле сервисов и типе узла. В Nmap Security Scanner выделяется несколько типов узлов [25], представленных в таблице 2.1. Каждому из данных типов узлов был сопоставлен коэффициент критичности (Criticality Coefficient, CC), принимающий значения от 0 до 1, также содержащийся в таблице 2.1.

Таблица 2.1 – Описание типов узлов, предоставляемых nmap, и их коэффициента критичности для типовой сетевой инфраструктуры

|  |  |  |
| --- | --- | --- |
| **Тип узла** | **Описание** | **CC** |
| Общего назначения | Эта категория содержит операционные системы общего назначения, такие как Linux и Windows. | 0,5 |
| Мост | Мост объединяет две или более подсетей в одну. Работает на более низком уровне, чем роутер. | 0,8 |
| Широкополосный маршрутизатор | Устройства этой категории подключают сеть к Интернету по кабелю, ADSL, оптоволоконному кабелю и т.д. Некоторые из этих устройств осуществляют трансляцию сетевых адресов, переадресацию портов и другие услуги. | 0,9 |
| Межсетевой Экран | Узлы данной категории осуществляют фильтрацию траффика, идущего в сеть и из неё. | 0,8 |
| Игровая консоль | Консоль для видеоигр, такая как Xbox или PlayStation | 0,2 |
| Сетевой концентратор | Объединяет сегменты сети, повторно транслируя весь трафик. Концентраторы отличаются от коммутаторов, которые выборочно передают пакеты только в соответствующие пункты назначения. | 0,5 |
| Балансировщик нагрузки | Осуществляет распределение входящего траффика по узлам сети, выполняющим одинаковые функции, для снижения нагрузки на отдельные устройства. | 0,4 |
| Мультимедийное устройство | Под эту категорию попадают все виды мультимедийного оборудования, в том числе музыкальные проигрыватели, телевизоры, проекторы и аудиосистемы. | 0,3 |
| PBX | Осуществляет перенаправление звонков на VoIP или телефоны сети общего пользования. | 0,6 |
| PDA | Категория устройств, к которым относятся карманные портативные компьютеры (КПК) | 0,5 |
| Телефон | Мобильные телефоны | 0,7 |
| Устройство питания | Различные источники питания, такие как источники бесперебойного питания и сетевые фильтры. | 0,2 |
| Принтер | Сетевые принтеры, включая принтеры со встроенным сервером печати | 0,4 |
| Сервер печати | Сервер, подключающий принтер к сети. | 0,4 |
| Прокси-сервер | Прокси любого типа, включая веб-прокси и другие серверы, которые кэшируют данные или понимают протоколы высокого уровня. | 0,6 |
| Сервер удаленного управления | Устройства, которые позволяют удаленно контролировать или управлять другим оборудованием. | 1 |
| Роутер | Устройства, соединяющие несколько сетей. Отличаются от концентраторов и коммутаторов, поскольку маршрутизируют пакеты между различными сетями, а не расширяют одну сеть. | 0,9 |
| Прочие устройства безопасности | Любое сетевое устройство, не попадающее в категорию «Межсетевые экраны». К ним относятся IDS, IPS и т.д. | 0,8 |
| Специализированное устройство | Если устройство не попадает ни в одну из других категорий, оно является специализированным. | 0,5 |
| Устройства хранения | Устройства хранения данных, такие как магнитные ленты и сетевые устройства хранения данных. | 1 |
| Коммутатор | Устройство, осуществляющее ретрансляцию пакетов канального уровня. | 0,4 |
| Телекоммуникационное устройство | Устройства, используемые телефонными системами, которые не являются PBX, как голосовая почта и ISDN. | 0,3 |
| Терминал | Устройство, главной целью которого является связь с терминальным сервером. | 0,8 |
| Терминальный сервер | Устройство, предоставляющее терминальные услуги клиентам сети. | 0,95 |
| VoIP адаптер | Устройства, преобразующие протоколы передачи голоса по IP в обычный телефонный трафик. | 0,4 |
| VoIP телефон | Телефон с поддержкой VoIP | 0,4 |
| WAP | Точки доступа, обеспечивающие беспроводное подключение к сети. | 0,75 |
| Веб-камера | Любое устройство, транслирующее изображение или видео. | 0,35 |

Каждому узлу графа сопоставляется список открытых портов и запущенных на них сервисов. Критичность компрометации узла складывается из критичности компрометации каждого из сервисов, запущенных на данном узле и умноженных на коэффициент критичности.

Для определения критичности узла необходимо задать уровень критичности каждого из сервисов. Разделим сервисы на группы:

* Web-сервисы;
* Системы управления базами данных;
* Сервисы удаленного управления рабочей станцией;
* Файловые сервисы;
* Почтовые сервисы;
* Остальные сервисы.

В таблице 2.2 приведена критичность каждой группы сервисов в терминах компрометации узла сети. Параметр критичности может принимать значения от 0 до 100

Таблица 2.2 – Стоимость групп сервисов

|  |  |
| --- | --- |
| **Группа** | **Стоимость** |
| Web-сервисы; | 75 |
| Системы управления базами данных; | 95 |
| Сервисы удаленного управления рабочей станцией; | 85 |
| Файловые сервисы; | 60 |
| Почтовые сервисы; | 40 |
| Остальные сервисы | 25 |

## Методика оценки защищенности сетевой инфраструктуры

Для оценки защищенности сетевой инфраструктуры необходимо провести оценку рисков компрометации каждого узла, а также значение нисходящего риска, который вычисляется как сумма рисков компрометации всех узлов, достижимых из текущего узла. Для оценки рисков каждого узла используется формула:

Где – коэффициент зависящий от типа узла, а – критичность сервиса, зависящая от принадлежности узла к одной из групп, определенных в п.2.1 данной работы, – сервис узла

После вычисления критичности каждого из узлов можно приступить к оценке нисходящего риска для каждого узла:

Где – оценка нисходящего риска - критичность попадания злоумышленника на узел , – узел графа, достижимый из , – критичность захвата узла , – подмножество достижимых узлов из .

Узел достижим из хотя бы 1 путь из в , *.*

Для подсчета необходимо определить множество . Для этого выполняется обход графа в глубину (алгоритм DFS), начиная от узла , и помечаются все достижимые узлы.

Уровень риска системы определяется, как сумма нисходящего риска каждого из узлов, что фактически означает следующее: насколько уязвима система, при осуществлении атаки на сеть с любого из узлов системы.

Уровень риска вычисляется следующим образом:

## Методика выбора защитных мер

Процесс выбора защитных мер опирается на показатель уровня риска системы. Методика выбора защитных мер заключается в поиске такой уязвимости , при удалении которой максимально снизится уровень риска системы, то есть:

В результате удаления уязвимости будут удалены все дуги графа атак, соединяющие любой узел с узлом посредством уязвимости . Такой набор ребер рассматривается как семейство ребер одной уязвимости и удаляется за одну итерацию. Использование данного метода позволит максимально снизить риск компрометации сети с любого из узлов системы, присутствующего в графе атак.

Так как в наивном исполнении построение графа атак занимает значительное время, были разработаны средства оптимизации процесса построения графа атак и предвычислений, призванные сократить время повторного вычисления нисходящего риска каждого узла.

Представим, что каждый узел исходного графа принадлежит подграфу одного из двух типов – компоненте сильной связности или N-арному дереву.

Ориентированный граф называется сильно связным, если любые два его узла сильно связны. Два узла и любого графа сильно связны, если существует ориентированный путь из в и ориентированный путь из в . Компонентами сильной связности орграфа называются его максимальные по включению сильно связные подграфы. Областью сильной связности называется множество узлов компоненты сильной связности.

Осуществим поиск областей сильной связности (обозначим их , например, с помощью алгоритма Косарайю, который использует двойной обход в глубину [26]:

Ориентированное N-арное дерево — ацикличный орграф (ориентированный граф, не содержащий циклов), в котором только один узел имеет нулевую степень захода (в него не ведут дуги), а все остальные узлы имеют степень захода не больше N. Узел с нулевой степенью захода называется корнем дерева, узлы с нулевой степенью исхода (из которых не исходит ни одна дуга) называются концевыми узлами или листьями. Обозначим их . Значение N может отличаться от дерева к дереву.

При этом в N-арное дерево включаются только те узлы, входящие дуги которых направлены от узлов того же дерева. Исключение может составлять только корневой узел (дополнительное условие).

В первую очередь производится поиск всех компонент сильной связности и соответствующих им областей сильной связности. Проиллюстрируем данный щаг на примере. Считаем, что все узлы имеют по 1 уязвимости, вследствие чего дуги не подписаны (рисунок 2.1).



Рисунок 2.1 – Пример ориентированного графа

Обозначим на графе компоненты сильной связности и N-арные деревья (рисунок 2.2). Компоненты сильной связности обозначены зеленым цветом, N-арные деревья – оранжевым.



Рисунок 2.2 – Иллюстрация поиска подграфов двух типов

Рассмотрим некоторые свойства полученных подграфов:

* Из определения компоненты сильной связности следует, что в ней существуют маршруты из любого узла компоненты в любой другой. Отсюда:

где – k-ая область сильной связности

Следовательно, для каждой области сильной связности достаточно посчитать единственный раз.

* Из определения компоненты сильной связности и N-арного дерева следует, что, попав в любую из данных компонент, гарантируется прохождение по всем узлам подграфа. При этом в N-арном дереве существует только один корневой узел, следовательно, вход в данный подграф возможен исключительно через него, что позволит пройти по всем узлам данного дерева. Следовательно, при достижении корневого узла такого дерева нет необходимости в пересчете критичности его узлов. Достаточно сделать это один раз:

– критичность захвата подграфа

* Дуги исходного графа делятся на 3 категории:
  + Дуги, принадлежащие компонентам сильной связности;
  + Дуги, принадлежащие N-арным деревьям;
  + Дуги, связывающие различные подграфы.

В связи с этим при удалении ребер возможны 3 ситуации:

1. Если ребро находилось в компоненте сильной связности или N-арном дереве, необходимо осуществить перераспределение узлов данной компоненты по новым подграфам сильной связности и N-арным деревьям, если удаление ребра повлекло изменение структуры подграфа. Также необходимо осуществить новые расчёты параметров и
2. Если ребро соединяло две компоненты, нет необходимости в пересчете параметра подграфов.

Исходя из вышеописанных свойств можно провести следующее преобразование: представим все компоненты сильной связности и N-арные деревья как узлы нового графа, которые включают в себя все входящие и все исходящие дуги исходного подграфа. При этом новое значение критичности узла высчитывается по формуле:

А новое значение угрозы попадания на узел

Где – k-ая область сильной связности

Полученный в результате граф, будет иметь следующий вид (рисунок 2.3):

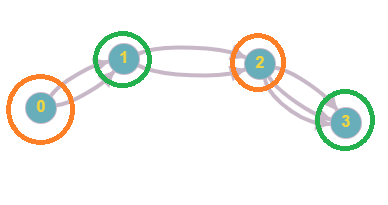


Рисунок 2.3 – Упрощенный вид графа

В результате такого преобразования граф избавляется от циклов, затрудняющих оценку защищенности системы, а также обеспечивается набором оптимизаций по вычислению показателей защищенности.

Таким образом, при определении уровня риска системы можно будет воспользоваться результатами предварительных расчетов что весьма критично, так рассматриваемая структура сетевой организации очень часто выглядит так, что . Следовательно, перерасчет критичности узлов и нисходящего риска на каждом этапе весьма затруднителен.

# Реализация системы оценки защищенности и выбора защитных мер

Для реализации автоматизированного программного комплекса, осуществляющего оценку защищенности сетевой инфраструктуры и выбора защитных мер на основе графа атак был выбран язык Python. Разрабатываемый комплекс был поделен на 4 основных компонента:

* Компонент обработки данных;
* Компонент оценки защищенности;
* Компонент выбора контрмер;
* Компонент визуализации.

## Архитектура системы оценки защищенности и выбора защитных мер

Архитектура реализованного комплекса выглядит следующим образом (рисунок 3.1).

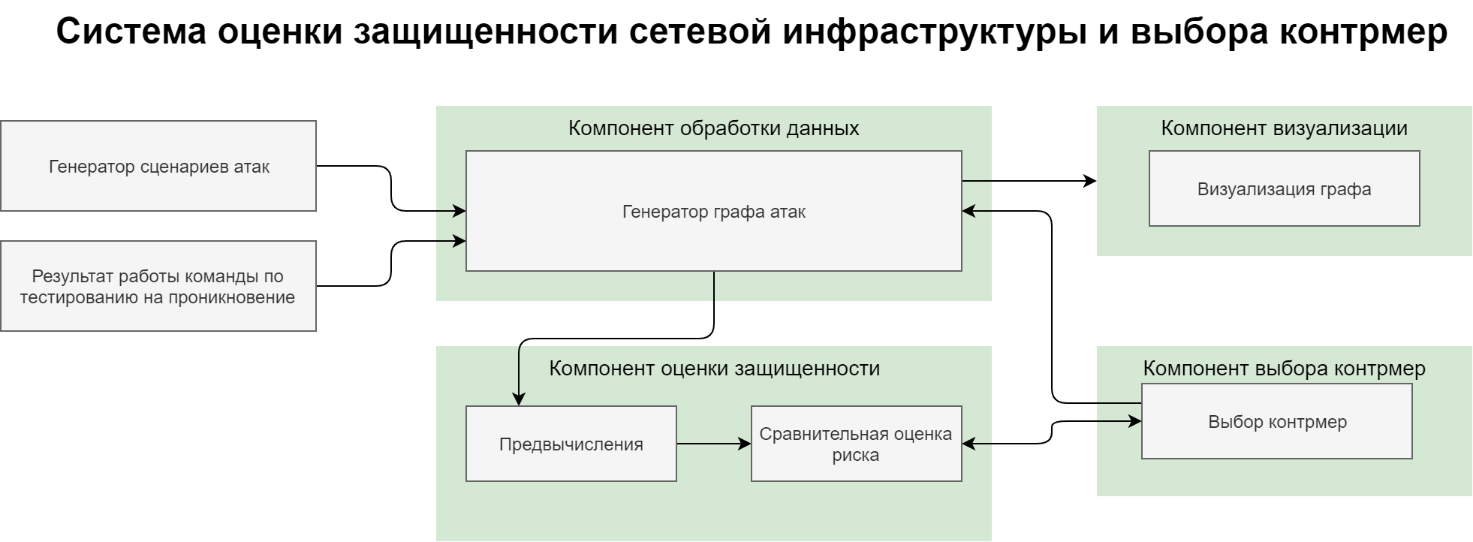


Рисунок 3.1 – Архитектура разработанной системы

Компонент обработки данных отвечает за преобразование входных данных и данных, поступающих с компонента выбора контрмер, в набор классов, реализующих операции над графом атак.

Компонент оценки защищенности производит вычисление основных показателей риска и производит сравнительную оценку текущего состояния и состояния, которому предшествовало удаление одной из существующих уязвимостей.

В компоненте выбора контрмер реализуются алгоритмы поиска уязвимости, при удалении которой максимально снизится уровень риска системы.

Компонент визуализации осуществляет отправку данных о графе атак на сервис 3vis, разработанный компанией NeoBIT для полноценной визуализации графа атак.

Разработанный программный комплекс осуществляет итеративный поиск оптимальных контрмер. Это значит, что на вход подаётся количество уязвимостей, которые необходимо удалить, а на выходе имеется набор пар где r – целевой узел, а c – одна из его уязвимостей, упорядоченные по приоритету устранения.

Например, рассмотрим граф атак, приведенный на рисунке 3.2.

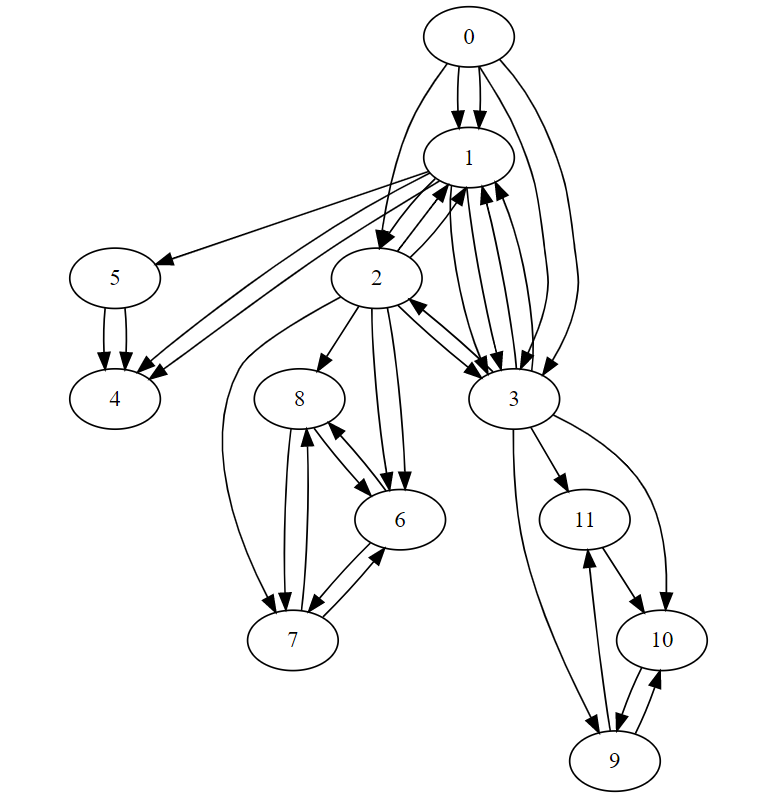


Рисунок 3.2 – Пример графа потенциальных атак

Вершины данного графа имеют порядковые номера от 0 до 11. В соответствии с номером вершины в таблице 3.1 определены критичности компрометации каждого из узлов графа и идентификаторы уязвимостей узлов графа.

Таблица 3.1 – Описание узлов графа и их уязвимостей

|  |  |  |
| --- | --- | --- |
| **Идентификатор узла** | **Показатель критичности** | **Идентификаторы уязвимостей** |
| 0 | 0 |  |
| 1 | 10 | ['CVE\_1\_0', 'CVE\_1\_1'] |
| 2 | 10 | ['CVE\_2\_0'] |
| 3 | 80 | ['CVE\_3\_0', 'CVE\_3\_1'] |
| 4 | 70 | ['CVE\_4\_0', 'CVE\_4\_1'] |
| 5 | 80 | ['CVE\_5\_0'] |
| 6 | 40 | ['CVE\_6\_0', 'CVE\_6\_1'] |
| 7 | 10 | ['CVE\_7\_0'] |
| 8 | 30 | ['CVE\_8\_0'] |
| 9 | 80 | ['CVE\_9\_0'] |
| 10 | 60 | ['CVE\_10\_0'] |
| 11 | 70 | ['CVE\_11\_0'] |

Узел 0 представляет собой узел атакующего, то есть узел, с которого проводилось построение графа. Идентификаторы уязвимостей имеют следующий формат:

CVE\_[идентификатор узла, на котором найдена уязвимость]\_[порядковый номер обнаруженной уязвимости].

Рассмотрим, как меняется уровень риска на протяжении поиска 5 наиболее критичных уязвимостей:

1. T = 3250;
2. T = 2700, c = CVE\_9\_0;
3. T = 2220, c = CVE\_1\_1;
4. T = 1860, c = CVE\_10\_0;
5. T = 1240, c = CVE\_11\_0;
6. T = 1000, c = CVE\_3\_1.

После устранения данных уязвимостей граф приобрел следующий вид (рисунок 3.3).

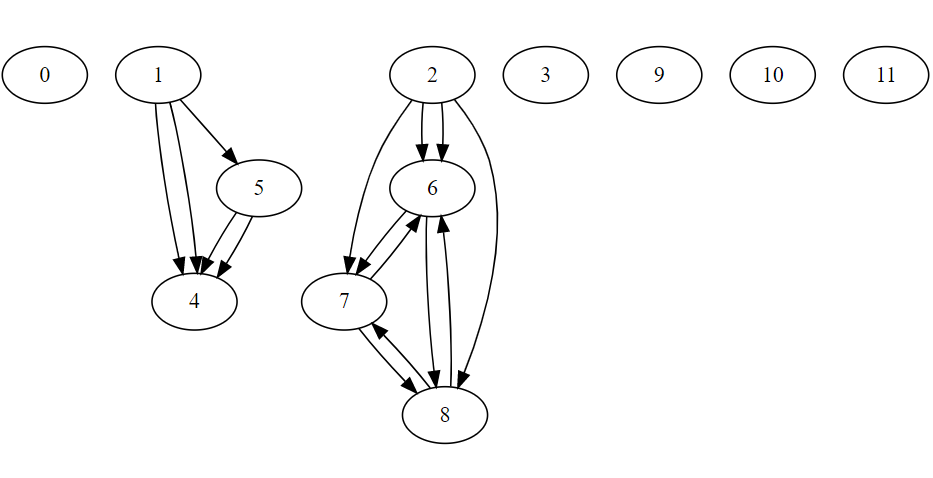


Рисунок 3.3 – Результат устранения 5 уязвимостей, максимизировавших уровень риска системы

Как видно из рисунка 3.3, удаление наиболее критических уязвимостей повлекло разложение графа на небольшие подграфы, благодаря чему значительно уменьшился уровень риска системы.

# Заключение

Анализ существующих методик оценки защищенности показал, что большинство методик не рассчитано на использование в процессе анализа без наличия такой дополнительной информации, как важность актива для бизнеса, его реальная стоимость и ущерб в результате компрометации, которые могут быть получены только с разрешения владельца актива. Также было замечено, что многие методики с точки зрения затрат на введение мер защиты, предпочитают устранять исключительно внешние уязвимости, чтобы, например, уменьшить процент покрытия атаки. Таким образом, они не учитывают потенциальные векторы атак, которые могут быть направлены от элементов сетевой инфраструктуры, не являющихся точками входа. При этом сохраняются все цепочки уязвимостей, расположенные в одном переходе от точек входа.

Появление новых сервисов и открытых портов на узлах сети может привести к возникновению новых точек входа, через которые злоумышленники смогут воспользоваться уже существующими цепочками уязвимостей, что подтверждает актуальность данной работы.

В качестве основной структуры для анализа был выбран граф атак, так как он позволяет максимально точно передать состояние исследуемой системы, взаимосвязи между узлами и сервисами.

В данной работе предлагается новый подход к решению проблемы выбора защитных мер и оценки защищенности сетевой инфраструктуры. Данный подход использует процесс оценки рисков на основе графов атак, что позволяет учесть топологию сети, найденные уязвимости и взаимодействие между узлами в процессе оценки. Таким образом, обеспечивается оптимальная последовательность действий, необходимых для уменьшения уровня риска всей исследуемой системы, а не только нисходящего риска от точек входа, что рассматривается в некоторых работах.

Для решения проблем наличия циклов и значительного времени построения графов атак используется ряд оптимизаций, не накладывающий никаких ограничений на исследуемый граф атак.

Реализованная система может успешно решать задачу оценки защищенности и поиска защитных мер и применяться как дополнение к системам автоматизированного тестирования на проникновение с последующей выработкой рекомендаций.

# Список использованных источников

1. Positive Technologies pentesters breach network perimeter at 92 percent of companies // PTSECURITY.COM: основной сайт Positive Technologies. – URL: https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019/ – (дата обращения 11.10.2019).
2. Criteria for Selecting an Information Security Risk Assessment Methodology: Qualitative, Quantitative, or Mixed // TCDI.COM: information security forum. – URL: https://www.tcdi.com/criteria-for-selecting-an-information-security-risk-assessment-methodology-qualitative-quantitative-or-mixed/. – (дата обращения 21.10.2019)
3. Брюховецкая Н.Е., Педерсен И.А. Vетодология оценки рисков предприятия//Стратегия и механизмы регулирования промышленного развития. – 2011. – С. 58.
4. Visintine V. Global information assurance certification paper// SANS Institute – 2003. – P. 13.
5. Caralli R.A., Stevens J.F., Young L.R., Wilson W.R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. – 2007. – P.9.
6. Peltier T. R. Information security risk analysis, Third Edition – New York: CRC Press, 2010. – P. 456.
7. Resources for Security Risk Analysis, ISO 17799 / BS7799 Security Policies & Security Audit // SECURITYAUDITOR.NET: сайт компании Risk Associates. – URL: https://www.securityauditor.net/. – (дата обращения 21.10.2019).
8. Information technology — Security techniques — Code of practice for information security management // ISO/IEC 17799. – 2005.
9. Fabbri J. Risk Scoring Methodology // RISKWATCH.COM: risk watch website. – URL: https://riskwatch.com/2019/07/31/risk-scoring-methodology/. – (дата обращения 25.10.2019)
10. Комплексное решение для управления информационной безопасностью // DSEC.RU: digital security company website. – URL: https://dsec.ru/press-release/digital-security-office-2005-kompleksnoe-reshenie-dlya-upravleniya-informatsionnoj-bezopasnostyu/. – (дата обращения 02.11.2019).
11. Астахов А.М. Искусство управления информационными рисками – Москва: ДМК Пресс, 2010 – С. 312.
12. CRAMM (CCTA Risk Analysis and Management Method) // MANAGEMENTMANIA.COM: management blogs. – URL: https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method. – (дата обращения 5.11.2019).
13. Дойникова Е. В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // Информационно-управляющие системы. – СПБ: Политехника, 2016. – С. 54
14. Ingols K. Practical attack graph generation for network defense // Proceedings of 22nd Annual Conference on the Computer Security Applications (Miami Beach, FL, 2006). – IEEE, 2006. – P. 121.
15. Жижелев А. В., Панфилов А. П., Язов Ю. К., Батищев Р. В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Известия вузов. Приборостроение. – 2003. – Т. 46. – № 7. – С. 22.
16. Kanoun W. Automated reaction based on risk analysis and attackers skills in intrusion detection systems // Proceedings of the Third International Conference on Risks and Security of Internet and Systems (28-30 Oct. 2008). – P. 117–124.
17. White Paper. 6 key risk management metrics for controlling cyber security // CDN2.HUBSPOT.NET: file sharing service. – URL: https://cdn2.hubspot.net/hubfs/91381/2019 Collateral/White Papers/Controlling Cyber Security/6 Key Risk Management Metrics for Controlling Cyber Security .pdf. – (дата обращения 15.11.2019).
18. The Center for Internet Security. The CIS Security Metrics // The Center for Internet Security. – 2009. – P.175.
19. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН. – СПб: Наука, 2013. – Вып. 26. – С. 54–68.
20. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 // NIST.GOV: an official website of the USA government. – URL: https://www.nist.gov/publications/complete-guide-common-vulnerability-scoring-system-version-20. – (дата обращения 15.11.2019).
21. Stan O., Bitton R., Ezrets M., Dadon M., Inokuchi M., Ohta Y., Yagyu T., Elovici Y., ShabtaiHeuristic A. Heuristic Approach Towards Countermeasure Selection using Attack Graph // DEEPAI.ORG: artificial intelligence researches. – URL: https://deepai.org/publication/heuristic-approach-towards-countermeasure-selection-using-attack-graphs. – (дата обращения 29.11.2019).
22. Cuppens F., Autrel F., Bouzida Y., Garcia J., Gombault S., Sans T. Anti-correlation as a criterion to select appropriate counter-measures in an intrusion detection framework // Annales Des Télécommunications. – 2006. – Vol. 61. – Iss. 1-2. – P.197-217
23. Lippmann, R. P. Validating and restoring defense in depth using attack graphs // MILCOM 2006 - 2006 IEEE Military Communications conference. – 2006.
24. Минаев В.А., Модестов А.А, Кухаренко Д.И. Основные теоретические положения структуризации частных показателей защиты информации с целью интегральной оценки защищенности информационно-телекоммуникационных систем // CYBERLENINKA.RU: исследования в области информационной безопасности. – URL: https://cyberleninka.ru/article/n/osnovnye-teoreticheskie-polozheniya-strukturizatsi i-chastnyh-pokazateley-zaschity-informatsii-s-tselyu-integralnoy-otsenki. – (дата обращения 14.12.2019).
25. Lyon G. Remote OS Detection // The Official Nmap Project Guide to Network Discovery and Security Scanning. – 2011.
26. Strongly connected components // GEEKSFORGEEKS.ORG: a computer science portal. – URL: https://www.geeksforgeeks.org/strongly-connected-components/. – (дата обращения 16.12.2019).

# Приложение А

Листинг компонента выбора контрмер

from time import time  
  
from networkx import MultiDiGraph, graph, is\_strongly\_connected  
from networkx.drawing.nx\_pydot import write\_dot  
  
from utils.graph\_search import GraphSearcher  
from utils.graph\_utils import get\_strongly\_connected\_components, subgraph\_criticality, map\_component\_edges, \  
 map\_component\_inside\_edges  
from utils.threat\_calc import ThreatCalculator  
  
  
class GraphOptimizer:  
  
 def \_\_init\_\_(self, multiDiGraph: MultiDiGraph):  
 # Nx MultiDiGraph used to compute threat  
 self.nxGraph = multiDiGraph  
 self.previousCopy = multiDiGraph.copy()  
 # Threat calculator with an ability to remember threat of node  
 self.threat\_calc = ThreatCalculator(self.nxGraph)  
  
 self.components\_index = 0  
 self.graph\_threat = 0  
 self.strong\_components = {}  
 self.links\_to\_strong\_components = {}  
 self.nodes\_threat = {}  
 self.strong\_components\_to\_update = set()  
 self.vulns = {}  
 self.nodes = []  
 self.edges = []  
  
 self.\_init\_graph()  
 pass  
  
 def \_init\_graph(self):  
 for node in self.nxGraph.nodes:  
 self.nodes.append(node)  
 self.vulns[node] = []  
  
 for edge in self.nxGraph.edges:  
 self.edges.append(edge)  
 if edge[2] not in self.vulns[edge[1]]:  
 self.vulns[edge[1]].append(edge[2])  
 pass  
  
 def save\_graph(self, name):  
 write\_dot(self.nxGraph, name)  
  
 def add\_node(self):  
 pass  
  
 def add\_edge(self, edge: list):  
 *"""  
 add edge to nx graph  
 :param edge: taple of source, destination and cve  
 :return:  
 """* self.nxGraph.add\_edge(edge[0], edge[1], edge[2], cve=edge[2])  
  
 def remove\_node(self, node):  
 *"""  
 Remove node from nx graph  
 :return:  
 """* self.nxGraph.remove\_node(node)  
 self.nodes.remove(node)  
 pass  
  
 def remove\_edge(self, edge: list):  
 *"""  
 remove edge from nx graph  
 :return:  
 """* self.nxGraph.remove\_edge(edge[0], edge[1], edge[2])  
  
 def remove\_cve(self, cve):  
 for edge in self.edges:  
 if edge[2] == cve:  
 self.remove\_edge(edge)  
  
 def \_link\_nodes\_to\_component(self, index: int):  
 # hash table, now we can find out, is current node in strong component or not  
 for node in self.strong\_components[index]['nodes']:  
 self.links\_to\_strong\_components[node] = index  
  
 def \_update\_component\_edges(self, index: int):  
 # Add all previous links to this node  
 edges\_in, edges\_out = map\_component\_edges(self.nxGraph, self.strong\_components[index]['nodes'])  
 edges\_inside = map\_component\_inside\_edges(self.nxGraph, self.strong\_components[index]['nodes'])  
  
 self.strong\_components[index]['edges\_inside'] = edges\_inside  
 self.strong\_components[index]['edges\_in'] = edges\_in  
 self.strong\_components[index]['edges\_out'] = edges\_out  
  
 def \_get\_strong\_components\_threat(self):  
 threat = 0.  
 for key, value in self.strong\_components:  
 threat += value['subgraph\_threat']  
  
 return threat  
  
 def \_extend\_nodes\_threat(self, new\_nodes\_threat):  
 for key, value in new\_nodes\_threat.items():  
 self.nodes\_threat[key] = value  
  
 def \_add\_strong\_component(self, strong\_component\_data: dict):  
 # need to get component by hash index, so used the identificator  
 self.strong\_components[self.components\_index] = strong\_component\_data  
  
 self.\_link\_nodes\_to\_component(self.components\_index)  
 self.\_update\_component\_edges(self.components\_index)  
 self.components\_index += 1  
  
 def create\_optimized\_component(self, component: list, criticality: float, threat: float):  
 # Seems that i don't need to mark edges here, because i can restore them from MultiDiGraph  
 # *TODO:Check, do i really need to keep list of nodes in component\_data* component\_data = {'threat': threat, 'criticality': criticality,  
 'subgraph\_threat': threat \* len(component), 'nodes': component}  
 self.\_add\_strong\_component(component\_data)  
  
 def \_remove\_strong\_component(self, component\_id):  
 *"""  
 Remove any information about strong component: node threat, links  
 :param component\_id:  
 :return:  
 """* component = self.strong\_components[component\_id]  
  
 for node in component['nodes']:  
 self.nodes\_threat.pop(node, None)  
 self.links\_to\_strong\_components.pop(node, None)  
  
 self.strong\_components.pop(component\_id, None)  
  
 def \_update\_strong\_component(self, component\_id: int):  
 *"""  
 Updates strong component after cve removal  
 :param component\_id:  
 :return:  
 """* component = self.strong\_components[component\_id]  
 subgraph = self.nxGraph.subgraph(component['nodes'])  
 is\_still\_strong = is\_strongly\_connected(subgraph)  
  
 if not is\_still\_strong:  
 # Remove previous component and get new if we can  
 self.\_remove\_strong\_component(component\_id)  
 # Find new components  
 strong\_components\_nodes = get\_strongly\_connected\_components(subgraph)  
 # Add new components to list of components  
 for component in strong\_components\_nodes:  
 self.\_workout\_strong\_component(component)  
  
 def \_update\_component\_params(self, component\_id: int):  
 *"""  
 Update parameters of components such as criticality and threat  
 :param component\_id:  
 :return:  
 """* # When cve is deleted, component can be deleted, or just change the threat  
 component = self.strong\_components[component\_id]  
 component\_threat = self.threat\_calc.calculate\_graph\_threat([component['nodes'][0]])  
 # Pre computed threat for all strong component nodes  
 for node in component['nodes']:  
 self.nodes\_threat[node] = component\_threat  
  
 component['threat'] = component\_threat  
 component['subgraph\_threat'] = component\_threat \* len(component['nodes'])  
  
 # We need to update those edges, cause we use it to compute the threat  
 # *TODO: measure the time for updating the edges. May be should change the mechanism to avoid this part* self.\_update\_component\_edges(component\_id)  
  
 def \_update\_nodes\_threat(self, node\_list: list):  
 self.strong\_components\_to\_update = set()  
 # *TODO: newly built strong components are calculated twice!* for node in node\_list:  
 if node in self.links\_to\_strong\_components:  
 self.strong\_components\_to\_update.add(self.links\_to\_strong\_components[node])  
 else:  
 self.nodes\_threat.pop(node, None)  
  
 def \_workout\_strong\_component(self, component):  
 calc = ThreatCalculator(self.nxGraph)  
 component\_criticality = subgraph\_criticality(self.nxGraph, component, component[0])  
 # we can take only 1 node from strong connected component and multiply it on component size  
 # *TODO: may be i should speed up the threat counting by using memorized\_calculate\_threat\_for\_node???* component\_threat = calc.calculate\_graph\_threat([component[0]])  
 # Pre computed threat for all strong component nodes  
 for node in component:  
 self.nodes\_threat[node] = component\_threat  
  
 self.create\_optimized\_component(component, component\_criticality, component\_threat)  
  
 def \_update\_after\_countermeasure(self, target):  
 new\_components = []  
 if target in self.links\_to\_strong\_components:  
 component\_id = self.links\_to\_strong\_components[target]  
 subgraph = self.nxGraph.subgraph(  
 self.strong\_components[component\_id]['nodes'])  
 is\_still\_strong = is\_strongly\_connected(subgraph)  
  
 if is\_still\_strong:  
 return  
 else:  
 self.\_remove\_strong\_component(component\_id)  
 # Find new components  
 strong\_components\_nodes = get\_strongly\_connected\_components(subgraph)  
 # Add new components to list of components  
 for component in strong\_components\_nodes:  
 new\_components.append(self.components\_index)  
 self.\_workout\_strong\_component(component)  
  
 searcher = GraphSearcher(self.previousCopy)  
 nodes\_to\_target = searcher.get\_sources\_to\_target\_node(target)  
  
 self.\_update\_nodes\_threat(nodes\_to\_target)  
 # Remove newly created component from update list  
 for index in new\_components:  
 self.strong\_components\_to\_update.remove(index)  
 # searcher = GraphSearcher(self.previousCopy)  
 # nodes\_to\_target = searcher.get\_sources\_to\_target\_node(target)  
 #  
 # # Update strong components  
 # if target in self.links\_to\_strong\_components:  
 # self.\_update\_strong\_component(self.links\_to\_strong\_components[target])  
 #  
 # # Update nodes and strong component threats  
 # self.\_update\_nodes\_threat(nodes\_to\_target)  
  
  
 def find\_countermeasure(self):  
 calc = ThreatCalculator(self.nxGraph, self.strong\_components, self.links\_to\_strong\_components)  
 # *TODO: make own countermeasure calculation based on threat saving mechanisms* cve, new\_threat, target = calc.find\_best\_countermeasure\_choice(self.nodes, self.vulns)  
 # *TODO: may be I should return full list of edges to avoid searching for them again* # Remove cve edges to {target}  
 self.remove\_cve(cve)  
 # optimize after deletion  
 # self.\_update\_after\_countermeasure(target)  
  
 threat = self.compute\_threat()  
 return cve, new\_threat, target  
  
 def deep\_copy(self):  
 *"""  
 Full copy of changeable parameters  
 :return:  
 """* graph = self.nxGraph.copy()  
 nodes\_threat = self.nodes\_threat.copy()  
 strong\_components = self.strong\_components.copy()  
 index = self.components\_index  
 links = self.links\_to\_strong\_components.copy()  
  
 return [graph, nodes\_threat, strong\_components,index, links]  
  
 def restore(self, params: list):  
 *"""  
 restoration of changeable parameters  
 :param params:  
 :return:  
 """* self.nxGraph = params[0]  
 self.nodes\_threat = params[1]  
 self.strong\_components = params[2]  
 self.components\_index = params[3]  
 self.links\_to\_strong\_components = params[4]  
  
 def intelligence\_find\_countermeasure(self):  
 deleted\_vuln\_threat\_reducion = {}  
 base\_threat = self.compute\_threat()  
 max\_reduction = -1  
 max\_cve = ""  
 computation\_time = 0.  
 # tmp\_graph = self.graph.copy()  
 #*TODO: change score counting from depth to starter* for node in self.vulns.keys():  
 for vuln in self.vulns[node]:  
 # Make copy of changeable params  
 deep\_copy\_params = self.deep\_copy()  
 edges\_to\_delete = []  
 for u, v, attrs in self.nxGraph.in\_edges(node, data=True):  
 if attrs['cve'] == vuln:  
 edges\_to\_delete.append((u,v))  
 for u,v in edges\_to\_delete:  
 self.remove\_edge([u, v, vuln])  
 # Optimization step  
  
 self.\_update\_after\_countermeasure(node)  
 self.threat\_calc = ThreatCalculator(self.nxGraph, False,  
 self.strong\_components, self.links\_to\_strong\_components)  
 start = time()  
 reduction = base\_threat - self.compute\_threat()  
 computation\_time += time() - start  
  
 deleted\_vuln\_threat\_reducion[vuln] = reduction  
  
 if reduction > max\_reduction:  
 max\_reduction = reduction  
 max\_cve = vuln  
 target = node  
 # Restoration of base state  
 self.restore(deep\_copy\_params)  
  
 print(f"Compute time: {computation\_time}")  
 return max\_cve, base\_threat - max\_reduction, target  
  
 def compute\_threat(self):  
 *"""  
 After optimization we know the threat of strong components subgraphs and we destroyed the circles  
 so we can start remembering the threat of current nodes  
 :return:  
 """* threat = 0.  
 compute\_node\_list = []  
 # Update Threat of strong component  
 for component in self.strong\_components\_to\_update:  
 self.\_update\_component\_params(component)  
  
 # Clearing components to update set  
 self.strong\_components\_to\_update.clear()  
 # Threat of nodes that dont belong to strong components  
 calc = ThreatCalculator(self.nxGraph, False, self.strong\_components, self.links\_to\_strong\_components)  
 # Calculate threat only for updated paths  
 # So if we computed it before and it didn't change, so we can use it again  
 for node in self.nodes:  
 if node not in self.nodes\_threat:  
 compute\_node\_list.append(node)  
 else:  
 threat += self.nodes\_threat[node]  
 # Now we compute threat only for NEWLY changed pathes  
 threat += calc.memorized\_calculate\_graph\_threat(compute\_node\_list)  
 # Now we need to summarize it with strong components threat  
 # for component in self.strong\_components.values():  
 # graph\_threat += component['subgraph\_threat']  
  
 calculated\_nodes\_threat = calc.get\_nodes\_threat()  
 self.\_extend\_nodes\_threat(calculated\_nodes\_threat)  
  
 return threat  
  
 def optimize(self):  
 start = time()  
 strong\_components\_nodes = get\_strongly\_connected\_components(self.nxGraph)  
 components\_detection = time()  
 #Precount  
 # self.graph\_threat = ThreatCalculator(self.nxGraph).calculate\_graph\_threat(self.nodes)  
 for component in strong\_components\_nodes:  
 self.\_workout\_strong\_component(component)  
  
 #print(f"Constructed strong components in {time() - start} seconds")

Листинг вспомогательных утилит

def generate\_graph(max\_nodes: int, max\_vulns\_per\_node: int, max\_compromized\_from\_one\_node: int, chance: float = 50):  
 *"""  
 Generates random attack graph  
 :param chance: from 0 to 100  
 :param max\_compromized\_from\_one\_node:  
 :param max\_vulns\_per\_node:  
 :param max\_nodes: nodes amount  
 :return:  
 """* # random.seed(time())  
 random.seed(10)  
 cur\_nodes\_amount = 1  
 step\_nodes\_count = 1  
 graph = MultiDiGraph()  
 nodes\_list = [0]  
 devices = [0]  
 vulns = []  
 map\_node\_vulns = {}  
 node\_vulns = {}  
  
 graph.add\_node(nodes\_list[0],weight=0)  
 while cur\_nodes\_amount < max\_nodes:  
 tmp\_nodes\_list = []  
 for node in nodes\_list:  
 nodes = []  
 if cur\_nodes\_amount == 1:  
 step\_nodes\_amount = random.randint(1, max\_compromized\_from\_one\_node)  
 else:  
 step\_nodes\_amount = random.randint(0, max\_compromized\_from\_one\_node)  
  
 for i in range(step\_nodes\_amount):  
 next\_node = cur\_nodes\_amount  
 cur\_nodes\_amount += 1  
 node\_vulns[next\_node] = []  
 nodes.append(next\_node)  
 graph.add\_node(next\_node,weight=random.randint(1,10)\*10)  
 tmp\_nodes\_list.append(next\_node)  
  
  
 devices.append(next\_node)  
 step\_vulns\_for\_node = random.randint(1, max\_vulns\_per\_node)  
  
 for j in range(step\_vulns\_for\_node):  
 threat\_level = random.randint(1, 10)  
 cur\_vuln = f"CVE\_{str(next\_node)}\_{j}"  
 node\_vulns[next\_node].append(cur\_vuln)  
 vulns.append(cur\_vuln)  
  
 #graph.add\_edge(node, cur\_vuln, weight=0)  
 graph.add\_edge(node, next\_node, key=cur\_vuln, cve=cur\_vuln)  
  
 for node\_first in nodes:  
 for node\_second in nodes:  
 if node\_first == node\_second:  
 continue  
 for vuln in node\_vulns[node\_second]:  
 if random.randint(0, 100) < chance:  
 graph.add\_edge(node\_first, node\_second, key=vuln, cve=vuln)  
 # for key, value in node\_vulns.items():  
 # for key\_2, value\_2 in node\_vulns.items():  
 # if key\_2 == key:  
 # continue  
 # for vuln\_name in value\_2:  
 # if random.randint(0, 100) < chance:  
 # graph.add\_edge(key, key\_2, cve=vuln\_name)  
 nodes\_list = tmp\_nodes\_list  
 if len(nodes\_list) == 0:  
 break  
 # cur\_nodes\_amount += len(tmp\_nodes\_list)  
 step\_nodes\_count = len(tmp\_nodes\_list)  
  
 return (graph, devices, node\_vulns)  
  
def remove\_edges\_with\_cve(graph: MultiDiGraph, cve, target):  
 tmp = []  
 for u,v in graph.in\_edges(target):  
 tmp.append([u,v])  
  
 for edge in tmp:  
 graph.remove\_edge(edge[0],edge[1],cve)  
  
def get\_strongly\_connected\_components(graph: DiGraph, min\_nodes\_in\_component: int = 2):  
 *"""  
  
 :param min\_nodes\_in\_component:  
 :param graph:  
 :return:  
 """* strong\_components = list(strongly\_connected\_components(graph))  
 complex\_components = []  
 for component in strong\_components:  
 if len(component) >= min\_nodes\_in\_component:  
 complex\_components.append(list(component))  
  
 return complex\_components  
  
def subgraph\_criticality(graph: MultiDiGraph, nodes: set, start\_node):  
 *"""  
  
 :param start\_node:  
 :param graph:  
 :param nodes:  
 :return:  
 """* assert len(nodes) != 0  
 sub\_graph = graph.subgraph(nodes)  
 calc = ThreatCalculator(sub\_graph)  
  
 return calc.calculate\_threat\_for\_node(start\_node)  
  
def subgraph\_threat(graph: MultiDiGraph, nodes: set, strong: bool = False):  
 *"""  
 Определение уровня угрозы для набора точек  
 :param strong:  
 :param graph:  
 :param nodes:  
 :return:  
 """* assert len(nodes) != 0  
 sub\_graph = graph.subgraph(nodes)  
 calc = ThreatCalculator(sub\_graph)  
 if strong:  
 return len(nodes) \* calc.calculate\_threat\_for\_node(list(nodes)[0])  
 else:  
 return calc.calculate\_graph\_threat(list(nodes))  
  
  
def get\_component\_out\_edges(graph: MultiDiGraph, nodes: list) -> list:  
 *"""  
 Return all out edges  
 :param graph:  
 :param nodes:  
 :return: list of out edges  
 """* out\_elems = []  
 for elem in nodes:  
 for u, v, key in graph.out\_edges(elem, keys=True):  
 if v not in nodes and (u, v, key) not in out\_elems:  
 out\_elems.append([u, v, key])  
 return out\_elems  
  
def get\_component\_in\_edges(graph: MultiDiGraph, nodes: list) -> list:  
 *"""  
 Return all out edges  
 :param graph:  
 :param nodes:  
 :return: list of out edges  
 """* in\_elems = []  
 for elem in nodes:  
 for u, v, key in graph.in\_edges(elem, keys=True):  
 if u not in nodes and (u, v, key) not in in\_elems:  
 in\_elems.append([u, v, key])  
 return in\_elems  
  
def map\_component\_edges(graph: MultiDiGraph, component):  
 *"""  
 We look for all outgoing edges to ANOTHER components or nodes  
 :param graph:  
 :param component:  
 :return:  
 """* return get\_component\_in\_edges(graph, component), get\_component\_out\_edges(graph, component)  
  
def map\_component\_inside\_edges(graph: MultiDiGraph, component):  
 *"""  
 We look for all outgoing edges to ANOTHER components or nodes  
 :param graph:  
 :param component:  
 :return:  
 """* inside\_edges = []  
 for node in component:  
 for edge in graph.edges(node, keys=True):  
 inside\_edges.append(edge)  
 return inside\_edges  
  
def get\_sources\_to\_target\_node(graph: MultiDiGraph, target) -> list:  
 in\_elems = []  
 for u, v in graph.in\_edges(target):  
 if v == target:  
 in\_elems

Листинг компонента визуализации

from time import time  
  
import requests  
import json  
  
from networkx import DiGraph  
  
'''  
Make link:  
https://3vis.neobit.ru/api/graph/link  
  
{"sourceId":7710,"targetId":7690,"pid":"503868d2-97f8-4274-b0f5-46034000803f"}  
  
Make node:  
need to get id:  
response['msg']['node']['id']  
'''  
class GraphCreationError(Exception):  
 def \_\_init\_\_(self, \*args, \*\*kwargs):  
 Exception.\_\_init\_\_(self, \*args, \*\*kwargs)  
  
  
class GraphVisualizer:  
 def \_\_init\_\_(self, graph\_name):  
 self.name = graph\_name  
 self.graph\_id = None  
 self.graph\_links = []  
 self.nodes\_map = {}  
 self.auth\_token = ("BEARER eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1NzcyOTk5ODgsImlhdCI6MTU3NDcwNzk4OCw"  
 "iaWQiOjUsInN1YiI6Im9ybHlfdGVzdGVyIn0.MI8itHOSF81GOKwjMgfXTSCztlceTd6reJHO33VeqP8")  
 def create\_graph(self):  
 r = requests.post('https://3vis.neobit.ru/api/projects', json={"name": self.name},  
 headers={"Authorization":self.auth\_token})  
  
  
 if r.status\_code != 200:  
 raise GraphCreationError("Graph was not created")  
  
 try:  
 response = json.loads(r.text)  
 except Exception as ex:  
 raise GraphCreationError(f"Graph creation response error: {ex}")  
  
 self.graph\_id = response['msg']['project']['id']  
  
 def delete\_graph(self):  
 r = requests.delete(f'https://3vis.neobit.ru/api/projects/{self.graph\_id}', json={"pid": self.graph\_id},  
 headers={"Authorization":self.auth\_token})  
  
  
 if r.status\_code != 200:  
 raise GraphCreationError("Graph was not deleted")  
  
 def add\_node(self, node\_name, node\_type):  
 node\_params = {  
 "node":  
 {  
 "name":node\_name,"type":node\_type  
 },  
 "pid": self.graph\_id,  
 "needCompare":False  
 }  
 st = time()  
 r = requests.post("https://3vis.neobit.ru/api/graph/node", json=node\_params,  
 headers={"Authorization":self.auth\_token})  
 fin = time() - st  
 if r.status\_code != 200:  
 raise GraphCreationError("Node '{node\_name}' type '{node\_type}' was not created")  
  
 try:  
 response = json.loads(r.text)  
 except Exception as ex:  
 raise GraphCreationError(f"Graph node creation response error: {ex}")  
  
 self.nodes\_map[node\_name] = response['msg']['node']['id']  
  
 def add\_link(self, first\_node\_name, second\_node\_name, cve):  
 link\_params = {"sourceId": self.nodes\_map[first\_node\_name], "targetId": self.nodes\_map[second\_node\_name],  
 "pid":self.graph\_id}  
 r = requests.post('https://3vis.neobit.ru/api/graph/link', json=link\_params,  
 headers={"Authorization":self.auth\_token})  
   
 try:  
 response = json.loads(r.text)  
 except Exception as ex:  
 raise GraphCreationError(f"Graph node creation response error: {ex}")  
  
 self.graph\_links.append((first\_node\_name, second\_node\_name, cve))  
  
 def read\_graph(self, graph: DiGraph):  
 self.create\_graph()  
 node\_type = 'ip'  
  
 for node in graph.nodes:  
 self.add\_node(node,node\_type)  
  
 for edge in graph.edges:  
 self.add\_link(edge[0],edge[1],'cve\_1')  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 vizual = GraphVisualizer("test\_graph")  
 vizual.create\_graph()  
 vizual.add\_node('test\_node', 'ip')  
 vizual.add\_node('test\_node\_2', 'ip')  
 vizual.add\_link('test\_node', 'test\_node\_2', 'cve-1')  
 vizual.delete\_graph()

Компонент оценки защищенности

from networkx import DiGraph, MultiDiGraph  
  
  
class ThreatCalculator:  
  
 # def \_\_init\_\_(self, graph: DiGraph):  
 # self.graph = graph.copy()  
 # self.visited\_nodes = []  
 # self.nodes\_threat = {}  
  
 def \_\_init\_\_(self, graph: MultiDiGraph, deep\_copy: bool = True,  
 strong\_components: dict = None, links\_to\_components: dict = None):  
 if deep\_copy:  
 self.graph = graph.copy()  
 else:  
 self.graph = graph  
 self.strong\_components = strong\_components  
 self.links\_to\_components = links\_to\_components  
 self.visited\_nodes = []  
 self.nodes\_threat = {}  
  
 def calculate\_threat\_for\_node(self, node: str) -> float:  
 self.visited\_nodes.append(node)  
 node\_threat = self.graph.nodes[node]['weight']  
 for u, v in self.graph.out\_edges(node):  
 if v not in self.visited\_nodes:  
 # self.visited\_nodes.append(v)  
 # node\_threat += self.graph[u][v]['weight'] + self.calculate\_threat\_for\_node(v)  
 node\_threat += self.calculate\_threat\_for\_node(v)  
 return node\_threat  
  
 def calculate\_graph\_threat(self, device\_nodes: list) -> float:  
 self.nodes\_threat = {}  
 threat = 0.  
 for node in device\_nodes:  
 self.visited\_nodes = []  
 tmp\_threat = self.calculate\_threat\_for\_node(node)  
 self.nodes\_threat[node] = tmp\_threat  
 threat += tmp\_threat  
  
 return threat  
  
 def set\_preset\_of\_nodes\_threat(self, nodes\_threat):  
 self.nodes\_threat = nodes\_threat  
  
 def get\_nodes\_threat(self):  
 return self.nodes\_threat  
  
 def memorized\_calculate\_threat\_for\_node(self, node: str) -> float:  
 *"""  
 We can afford recursion with memory, cause we distracted all strong components in our graph  
 :param strong\_components:  
 :param node:  
 :return:  
 """* self.visited\_nodes.append(node)  
  
 node\_threat = self.graph.nodes[node]['weight']  
 for u, v in self.graph.out\_edges(node):  
 if v not in self.visited\_nodes:  
 try:  
 # If v is in strong component ->  
 component = self.strong\_components[self.links\_to\_components[v]]  
  
 for elem in component['nodes']:  
 self.visited\_nodes.append(elem)  
  
 if u in component['nodes']:  
 node\_threat = component['criticality']  
 else:  
 node\_threat += component['criticality']  
  
 for in\_node, out\_node, cve in component['edges\_out']:  
 if out\_node not in self.visited\_nodes:  
 node\_threat += self.memorized\_calculate\_threat\_for\_node(out\_node)  
  
 continue  
 except KeyError:  
 pass  
  
 node\_threat += self.memorized\_calculate\_threat\_for\_node(v)  
  
 return node\_threat  
  
 def memorized\_calculate\_graph\_threat(self, device\_nodes: list) -> float:  
 threat = 0.  
 self.nodes\_threat = {}  
 for node in device\_nodes:  
 if node in self.links\_to\_components:  
 # threat += self.strong\_components[self.links\_to\_components[node]]['threat']  
 continue  
 else:  
 self.visited\_nodes = []  
 tmp\_threat = self.memorized\_calculate\_threat\_for\_node(node)  
 self.nodes\_threat[node] = tmp\_threat  
 threat += tmp\_threat  
  
 return threat  
  
 def find\_best\_countermeasure\_choice(self, device\_nodes: list, node\_vulns: dict) -> (str, float):  
 deleted\_vuln\_threat\_reducion = {}  
 base\_threat = self.calculate\_graph\_threat(device\_nodes)  
 max\_reduction = -1  
 max\_cve = ""  
 computation\_time = 0.  
 # tmp\_graph = self.graph.copy()  
 #*TODO: change score counting from depth to starter* for node in node\_vulns.keys():  
 for vuln in node\_vulns[node]:  
  
 base\_graph = self.graph.copy()  
 edges\_to\_delete = []  
 for u, v, attrs in self.graph.in\_edges(node, data=True):  
 if attrs['cve'] == vuln:  
 edges\_to\_delete.append((u,v))  
 for u,v in edges\_to\_delete:  
 self.graph.remove\_edge(u,v,key=vuln)  
  
 start = time()  
 reduction = base\_threat - self.calculate\_graph\_threat(device\_nodes)  
 computation\_time += time() - start  
 deleted\_vuln\_threat\_reducion[vuln] = reduction  
  
 if reduction > max\_reduction:  
 max\_reduction = reduction  
 max\_cve = vuln  
 target = node  
  
 self.graph = base\_graph  
  
 print(f"Computation time: {computation\_time}")  
 return max\_cve, base\_threat - max\_reduction, target  
  
 def get\_list\_of\_compromised\_nodes(self, nodes: list):  
 self.visited\_nodes = []  
  
 for n in nodes:  
 self.get\_connections(n)  
  
 return self.visited\_nodes  
  
 def get\_connections(self, node):  
 self.visited\_nodes.append(node)  
 for u, v in self.graph.out\_edges(node):  
 if v not in self.visited\_nodes:  
 self.get\_connections(v)