МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование кафедры)
01.03.02 Прикладная математика и информатика
(код и наименование направления подготовки, специальности)
Системное программирование и компьютерные технологии
(направленность (профиль)/специализация

БАКАЛАВРСКАЯ РАБОТА

на тему **Исследование и разработка средств тестирования веб-сайтов на уязвимости**

Студент	И.В. Смирнов	
	(И.О. Фамилия)	(личная подпись)
Руководитель	С.В. Баумгертнер	
	(И.О. Фамилия)	(личная подпись)
Консультанты	Н.В. Андрюхина	
	(И.О. Фамилия)	(личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент, А.В. Очеповский _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2019

АННОТАЦИЯ

Тема: «Исследование и разработка средств тестирования веб-сайтов на уязвимости».

Целью ВКР является исследование и разработка средств тестирования веб-сайтов на уязвимости.

Объект – обеспечение безопасности веб-сайтов.

Предмет – средства тестирования веб-сайтов на уязвимость.

В данной выпускной квалификационной работе исследуются угрозы и уязвимости веб-сайтов. Анализируются результаты тестирования веб-сайтов на уязвимости.

Структура ВКР состоит из введения, трех разделов, выводов и списка использованных источников.

Во введении описывается актуальность проводимого исследования, формулируется цель и ставятся задачи, которые необходимо решить.

В первой главе приводится анализ уязвимостей веб-сайтов.

Во второй главе рассматривается процесс разработки алгоритма защиты веб-сайта.

В третьей главе рассматривается процесс тестирования и внедрения алгоритма защиты веб-сайта.

Бакалаврская работа состоит из пояснительной записки на 46 страницах, включающей 14 рисунков, 31 источников и 1 приложение.

ABSTRACT

This graduation work deals with estimating the website's vulnerability.

The aim of the work is to is to study and develop tools for testing websites for vulnerabilities.

The object of the graduation work is the security of websites.

The subject of the graduation work is the protection of web site security.

The security of information websites, first of all, refers to a state of all components, which provide protection against possible threats at the required level.

Web application security is one of the most pressing issues in the context of information security. As a rule, most of the websites available on the Internet have various kinds of vulnerabilities and are constantly under attack. We give full coverage to the main threats to information security of web applications.

The structure of the graduation work consists of an introduction, three chapters, conclusions and a list of references.

The introduction describes the relevance of the study, formulates the goal and sets the tasks that need to be addressed.

The first chapter provides an analysis of website vulnerabilities.

The second chapter describes the process of a website security algorithm development.

The third chapter describes the process of testing and implementing a website security algorithm.

This graduation work is on 46 pages, includes 14 figures, the list of 31 sources and 1 appendix.

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ, ТЕРМИНОВ И СОКРАЩЕНИЙ

КАИС КРО – комплексная автоматизированная информационная система каталогизации ресурсов образования;

ИСПД– информационная система персональных данных;

SPP– Standart Paralell Port;

EPP – Enhanced Parallel Port;

ECP– Extended Capabilities Port);

АРМ – автоматизированное рабочее место;

ПО – программное обеспечение;

ЛВС – локально-вычислительная система;

VLAN– Virtual Local Area Network;

TCP– TRANSMISSION CONTROL PROTOCOL;

ADSL– Asymmetric Digital Subscriber Line;

ISDN – Integrated Services Digital Network;

SONET – Synchronous Optical NETworking;

ARCNET – Attached Resource Computer NETwork;

ATM – Asynchronous Transport Mode;

DCAP – Data Link Switching Client Access Protocol;

HDLC – High-Level Data Link Control;

LLDP – Link Layer Discovery Protocol;

PPP – Point-to-Point Protocol;

PPTP– Point-to-Point Tunneling Protocol;

RPR IEEE 802.17– Resilient Packet Ring;

IPv6 – Internet Protocol version 6;

IPsec– Internet Protocol Security.

ВВЕДЕНИЕ

Под безопасностью информации веб-сайтов, прежде всего, понимается такое состояние всех компонент, при котором обеспечивается защита от возможных угроз на требуемом уровне.

Безопасность веб-приложений — один из наиболее острых вопросов в контексте информационной безопасности. Как правило большинство веб-сайтов, доступных в Интернете, имеют различного рода уязвимости и постоянно подвергаются атакам. В разделе будут рассмотрены основные угрозы информационной безопасности веб-приложений.

В первую очередь это несет угрозу работоспособности сайта. Во вторую, но не менее важную, — сохранность пользовательских данных. Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании.

Актуальность работы обусловлена повышенными требованиями к информации и разнообразием атак на информацию, а также вреда от них.

Объект исследования – обеспечение безопасности веб-сайтов.

Предмет исследования – средства тестирования веб-сайтов на уязвимость.

Целью работы является исследование и разработка средств тестирования веб-сайтов на уязвимости.

Задачи работы:

- анализ угроз;
- классификация угроз;
- построение модели угроз;
- анализ современных технологий и систем защиты информации веб-сайтов;
- построение системы защиты информационных ресурсов в облачных сервисах;
- исследование оптимизации выбора используемых программно-аппаратных средств защиты информации веб-сайтов.

Практическая значимость проведенного исследования – позволяет на приведенном примере разработать типовые рекомендации по защите безопасности веб-сайтов.

Методы исследования – анализ, моделирование.

Работа состоит из введения, трех разделов, заключения, списка используемых источников и одного приложения.

В первой главе выполнен обзор основных уязвимостей веб-сайтов.

Во второй главе проанализированы алгоритмы атак веб-сайтов.

В третьей разработанная система моделирования атак веб-сайтов.

1 ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ

1.1 Общие сведения о безопасности веб-сайтов

Безопасность веб-приложений — один из наиболее острых вопросов в контексте информационной безопасности. Как правило большинство веб-сайтов, доступных в Интернете, имеют различного рода уязвимости и постоянно подвергаются атакам. В разделе будут рассмотрены основные угрозы информационной безопасности веб-приложений.

В первую очередь это несет угрозу работоспособности сайта. Во вторую, но не менее важную, — сохранность пользовательских данных. Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании.

Хакеры используют сайт для атак на другие ресурсы, в качестве опорного плацдарма, для рассылки спама или проведения DoS атак. Ваш сайт блокируют поисковики и браузеры, теряются пользователи.

Атака на веб-сайт в корпоративной среде может является т.н. точкой входа в корпоративную сеть компании.

Атаки на системы электронной коммерции могут быть использованы для совершения мошеннических действий, похищения клиентских баз и т.д.

Также, все эти атаки могут быть нацелены на дальнейшее «заражение» пользователей сайта, например, с помощью т.н. эксплоит-паков — средств эксплуатации уязвимостей браузеров и их компонентов, в том числе и с применением социотехнических векторов атаки.

По данным Kaspersky Security Network только за второе полугодие 2018 года:

Решения «Лаборатории Касперского» отразили 962 947 023 атаки, которые проводились с интернет-ресурсов, размещенных в 187 странах мира.

Зафиксировано 351 913 075 уникальных URL, на которых происходило срабатывание веб-антивируса.

Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на компьютерах 215 762 пользователей.

Атаки шифровальщиков отражены на компьютерах 158 921 уникального пользователя.

Нашим файловым антивирусом зафиксировано 192 053 604 уникальных вредоносных и потенциально нежелательных объекта.

Продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено:

1 744 244 вредоносных установочных пакета;

61 045 установочных пакетов мобильных банковских троянцев;

14 119 установочных пакетов мобильных троянцев-вымогателей.

Исходя из вышесказанного актуальной является задача определения защищенности веб-сайта с последующей разработкой мер безопасности.

Под уровнем исходной защищенности КАИСКРО понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик КАИСКРО[4]. Показатели исходной защищенности КАИС КРО представлены в таблице 1.1. Показатели защищенности определены в соответствии с пунктом 2 методического документа ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», таблица 1.2

Таблица 1.1 – Показатели исходной защищенности КАИС КРО

№ п/п	Технические и эксплуатационные характеристики КАИС КРО	Уровень защищенности
1	2	3
1.	По территориальному размещению – распределенная ИСПДн, развернутая в пределах города	низкий
2.	По наличию соединения с сетями общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования;	низкий

Продолжение таблицы 1.1

№ п/п	Технические и эксплуатационные характеристики КАИС КРО	Уровень защищенности
1	2	3
3.	По встроенным (легальным) операциям с записями баз персональных данных – модификация, передача	низкий
4.	По разграничению доступа к персональным данным – к ИСПДн имеет доступ определенный перечень сотрудников	средний
5.	По наличию соединений с другими базами персональных данных иных информационных систем персональных данных – ИСПДн, в которой используется несколько баз ПДн, принадлежащих одной организации	средний
6.	По уровню обобщения (обезличивания) персональных данных – ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	средний
7.	По объему персональных данных, которые предоставляются сторонним пользователям КАИС КРО без предварительной обработки – ИСПДн предоставляющая часть ПДн	средний

Таким образом, КАИС КРО имеет низкий уровень защищенности (57,14% характеристик КАИС КРО соответствуют уровню «средний», 42,86% [2] характеристик соответствуют уровню «низкий») и числовой коэффициент Y1=10.

Таблица 1.2 – Объекты воздействия

	Наименование	Объект воздействия	Особенности	Важность ресурса
1	2	3	4	5
Д.1	АРМ	Жесткие магнитные диски (встроенные)	Может содержать защищаемые данные	средняя
		Оперативная память	Защищаемые данные уничтожается сразу после отключения питания	средняя
		Кэш-память, буферы ввода-вывода		средняя
		Видеопамять		низкая
		Монитор	Память объекта предназначена только для выполнения определенных задач данного устройства	низкая
		Клавиатура		низкая
		Принтер		низкая
		Привод магнитных и оптических дисков		низкая
		Порты ввода/вывода для подключения периферийных устройств		низкая
Д.2	Сервер	Жесткие магнитные диски (встроенные)	Содержит весь массив защищаемых данных	очень высокая
		Оперативная память	Серверы работают круглосуточно, поэтому защищаемая информация не уничтожается	высокая
		Кэш-память, буферы ввода-вывода		высокая
		Видеопамять		низкая
		Монитор	Память объекта предназначена только для выполнения определенных задач данного устройства	низкая
		Привод магнитных и оптических дисков		низкая
		Порты ввода/вывода для подключения периферийных устройств		низкая
Д.3	Отчуждаемые носители информации	Флеш-накопители, оптические диски	Может содержать любые защищаемые данные (в виде каких-либо отчетов, выборки и т.д.)	средняя
		Распечатанная документация и др. материальные носители видовой информации		средняя

Продолжение таблицы 1.2

	Наименование	Объект воздействия	Особенности	Важность ресурса
1	2	3	4	5
Д.4	Линии связи и коммутационное оборудование	Совокупность средств передачи данных – коммутаторы	Содержит защищаемые данные при информационном обмене и передаче служебной информации	средняя

В зависимости от объекта воздействия, угрозы доступа (проникновения) в программную среду КАИС КРО подразделяются на угрозы непосредственного и удаленного доступа

Описание внешних нарушителей приведено в таблице 1.3.

Таблица 1.3 – Классификация внешних нарушителей

Категория (вид) нарушителя, обозначение	Квалификация	Техническая оснащенность	Степень опасности
1	2	3	4
Лица, находящиеся за пределами контролируемой зоны и использующие технические средства ведения разведки и/или закладочные устройства – А.1.1	Высокая. Опыт получен в процессе профессиональной деятельности	Технические средства перехвата без модификации компонентов системы	Низкая
Лица, получившие доступ к информационным ресурсам КАИС КРО из внешних сетей телекоммуникаций, в том числе ССОП- А.1.2	Может быть высокой в случае профессиональной деятельности нарушителя, а также в случае сговора группы нарушителей (например, с целью финансовой выгоды)	Программно-технические средства воздействия с возможностью модификации компонентов системы	Высокая

Возможности и потенциальная опасность противоправных действий внутренних нарушителей раскрыты в таблице 1.4.

Таблица 1.4 – Классификация внутренних нарушителей

№ п/п	Категория нарушителя	Выполняемые функции в КАИС КРО	Возможности	Степень опасности
1	2	3	4	5
1.	Лицо, имеющее санкционированный доступ в КЗ, в которой размещены технические средства КАИС КРО, но не имеющее прав доступа к защищаемым ресурсам - А.2.1	Обеспечение нормального функционирования технических средств КАИС КРО	– располагает фрагментами информации, содержащими ПДн; – располагает фрагментами информации о топологии ИСПДн, об используемых коммуникационных протоколах и сервисах; – располагает именами зарегистрированных пользователей; – способен изменять конфигурацию и осуществлять несанкционированное подключение к техническим средствам ИСПДн; – способен вносить программно-аппаратные закладки.	Низкая
2.	Лицо, обеспечивающее поставку, сопровождение и ремонт технических средств КАИС КРО - А.2.2	Поставка, сопровождение и ремонт средств вычислительной техники	– обладает возможностью внесения закладок в технические средства КАИС КРО; – может располагать фрагментами информации о топологии ИСПДн и о тех. средствах.	Низкая

Продолжение таблицы 1.4

№ п/п	Категория нарушителя	Выполняемые функции в КАИС КРО	Возможности	Степень опасности
1	2	3	4	5
3.	Зарегистрированный пользователь КАИС КРО, имеющий права доступа к защищаемым ресурсам с рабочего места (оператор) – А.2.3.	Чтение, поиск, ввод новых данных, извлечение данных в КАИС КРО.	– располагает фрагментами информации о топологии ИСПДн, об используемых коммуникационных протоколах и сервисах; – способен изменять конфигурацию и осуществлять несанкционированное подключение к техническим средствам ИСПДн; – способен вносить программно-аппаратные закладки; – имеет учетную запись в системе; – имеет доступ к некоторому массиву ПДн.	Средняя

Лицо из перечисленных в таблице выше категорий, в соответствии со степенью опасности (низкая – средняя – высокая), может нанести меньший или больший ущерб системе и реализовать ту или иную угрозу безопасности информации КАИС КРО.

Вредоносные программы (обозначение «А» в указанной ниже таблице 6.5) можно разделить на классы по принципу функционирования:

- загрузочные (А.3.1);
- файловые (А.3.2);
- сетевые (А.3.3);
- прочие вредоносные программы (А.3.4).

Основными действиями, выполняемыми вредоносными программами, являются:

– уничтожение информации в секторах винчестера;
– исключение возможности загрузки операционной системы;
– искажение кода загрузчика;
– форматирование логических дисков винчестера;
– закрытие доступа к COM и LPT-портам;
– замена символов при печати текстов;
– подергивания экрана;
– изменение метки диска;
– создание псевдосбойных кластеров;
– создание звуковых и (или) визуальных эффектов;
– порча файлов данных;
– перезагрузка компьютера;
– вывод на экран разнообразных сообщений;
– отключение периферийных устройств;
– изменение палитры экрана;
– заполнение экрана посторонними символами или изображениями;
– погашение экрана и перевод в режим ожидания ввода с клавиатуры;
– шифрование секторов винчестера;
– выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
– уменьшение объема оперативной памяти;
– вызов печати содержимого экрана;
– блокирование записи на диск;
– уничтожение таблицы разбиения (DiskPartitionTable);
– блокирование запуска исполняемых файлов;
– блокирование доступа к винчестеру.

По способу проникновения в КАИС КРО вредоносные программы можно разделить на:

– распространяемые при использовании отчуждаемых носителей информации (оптические компакт-диски, флеш-накопители);

– распространяемые по сети (локальной, корпоративной, глобальной).

Наличие в КАИС КРО вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

Уязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Уязвимости используемого в КАИС КРО программного обеспечения рассмотрены с привязкой к техническим средствам КАИСКРО (таблица 1.6):

Таблица 1.6 – Используемое программное обеспечение

Техническое средство	Операционная система	Прикладное программное обеспечение
1	2	3
АРМ пользователей и персонала КАИС КРО	MS Windows 2000 MS Windows XP MS Windows Vista MSWindows 7	MS Office 2003; MS Office 2007; WinRar 3.5-3.8; Outlook Express; IE 6-7; ABBYYFinereader 9.0 Corporate Edition RUS; Adobe Acrobat 7-9; AVP Kaspersky 6.0; АРМ «ПараграфОУ/ДОУ/Колледж»; АРМ КАИС КРО; MapInfo 9.5; Правовые системы.
Серверы баз данных подсистемы «Параграф»	WindowsServer 2003 SP2	СУБД Firebird.

Продолжение таблицы 1.6

Техническое средство	Операционная система	Прикладное программное обеспечение
1	2	3
Сервер баз данных подсистемы портал «Петербургское образование»	LinuxUbuntuServer 11.04	VMWareESXi 4.0; СУБД MySQL v.5.5.10.
Сервер приложений подсистемы портал «Петербургское образование»	LinuxUbuntuServer 11.04	VMWareESXi 4.0; FTP-серверProFTPD v.1.3.2; Веб-сервер Lighttpd v.1.4.26; SMTP-сервер Postfix v.2.7; POP3-сервером Dovecot v.1.2.12.
Сервер резервирования	LinuxUbuntuServer 11.04	VMWareESXi 4.0.
Сервер ВКС	LinuxUbuntuServer 11.04	VMWareESXi 4.0; ВКС «ВидеоМост».

Данные об уязвимостях разрабатываемого и распространяемого на коммерческой основе прикладного программного обеспечения собираются, обобщаются и анализируются в базе данных CVE (http://cve.mitre.org/cve/). Степень критичности уязвимостей зависит от типа воздействия на приложение или систему, наличия исправления или временного решения, представленного производителем, наличия эксплоита и возможности массовой эксплуатации уязвимости. Таким образом, для характеристики уязвимости применяется следующая градация:

- высокая – уязвимость, которая может привести к нарушению конфиденциальности, целостности и доступности пользовательских данных или целостности и доступности вычислительных ресурсов;
- средняя – уязвимость, которая в значительной степени смягчается такими факторами, как конфигурационные настройки по умолчанию, аудит или трудность ее применения;
- низкая – уязвимость очень сложна для использования или ее воздействие минимально.

1.2 Исследование уязвимостей веб-сайтов

Существует несколько методов для оценки риска. Важно, чтобы организация пользовалась наиболее удобным и внушающим доверие методом, приносящим воспроизводимые результаты.

Оценивание рисков будет производиться экспертным путем на основе анализа ценности активов, возможности реализации угроз и использования уязвимостей, определенных в предыдущих пунктах. Для оценивания предлагается таблица с заранее предопределенными «штрафными баллами» для каждой комбинации ценности активов, уровня угроз и уязвимостей (таблица 1.7).

Таблица 1.7. Уровень угроз и уязвимостей

	Уровни угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

В случае определения уровня уязвимости из результатов аудита или самооценки для различных процессов и при наличии экспертных оценок уровня соответствующих угроз и ценности активов можно получить меру риска ИБ для каждого процесса (таблица 1.8).

Таблица 1.8. Результаты оценки рисков информационным активам организации

Риск	Актив	Ранг риска
1	2	3
Кража	Сервера	6
Несанкционированный доступ	Базы данных	6
Отсутствие надзора за работой лиц, приглашенных со стороны	Базы данных	6
Сбои / ошибки	Базы данных	6
Несанкционированный доступ	Сервера	5
Сбои / ошибки	Сервера	5

Продолжение таблицы 1.8

Риск	Актив	Ранг риска
1	2	3
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц	Базы данных	5
Сбои / ошибки	Программное обеспечение	5
Отсутствие надзора за работой лиц, приглашенных со стороны	Документы	5
Кража	Персональный компьютер	5
Несанкционированный доступ	Персональный компьютер	5
Сбои / ошибки	Персональный компьютер	5
Несанкционированный доступ	Программное обеспечение	4
Несанкционированный доступ	Документы	4
Сбои / ошибки	Документы	4

Исходя из данных таблицы, наибольшему риску подвержены сервера и базы данных.

1.3 Основные типы уязвимостей

Основными коммутирующими устройствами, использующиеся в ЛВС локальных составных частей КАИС КРО, являются коммутаторы D-Link, LynkSys, ASUS и другие.

Взаимодействие в ЛВС ОУ на канальном уровне осуществляется по стандартным протоколам IEEE 802.3. Сегментирование пользователей на виртуальные частные сети (VLAN) не применяется. Механизмов повышения отказоустойчивости и доступности не используется. Все рабочие станции и серверы, входящие в состав КАИС КРО, подключаются непосредственно к коммутаторам доступа образовательных учреждений.

Сетевое взаимодействие всех технических средств КАИС КРО основано на протоколах TCP/IP.

TCP - базовый сетевой протокол, в настоящее время используемый в большинстве сетевых компьютерных систем. Многие производители включают поддержку этого протокола в свои программы, которые могут быть в различной степени уязвимы. Кроме того, любые сетевые службы или приложения, опирающиеся на TCP подключения, тоже подвержены нападениям, причем опасность нападения зависит, прежде всего, от продолжительности TCP сеанса.

Уязвимости протоколов сетевого взаимодействия (обозначение «В.2» в указанных ниже таблицах 1.8 - 1.9) связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Характеристика этих уязвимостей представлена в таблице 1.9.

Таблица 1.9 – Уязвимости протоколов сетевого взаимодействия

Протокол	Назначение	Характеристика уязвимости
1	2	3
FTP	Передача файлов по сети	Аутентификация на базе открытого теста Наличие дополнительных открытых портов
TCP	Для осуществления сетевого взаимодействия	Отсутствует механизм проверки корректности заполнения служебных заголовков пакета
IP	Для осуществления сетевого взаимодействия	Адресация узлов на базе открытого текста
UDP	Для осуществления сетевого взаимодействия	Отсутствует механизм предотвращения переполнения буфера и подтверждения доставки передаваемого пакета
DNS	Для осуществления сетевого взаимодействия	Отсутствует средство проверки аутентификации полученных данных от источника
SNMP	Для осуществления сетевого взаимодействия	Отсутствует поддержка аутентификации заголовков сообщений
ARP	Для осуществления сетевого взаимодействия	Аутентификация на основе открытого текста
RIP	Протокол обмена маршрутной информацией	Отсутствует аутентификация отправителя управляющего

		сообщения

Уязвимости, вызванные недостатками организации ТЗИ от НСД в КАИС КРО (обозначение «В.3» в указанных ниже таблицах 6.3-6.6) представлены в таблице 1.10.

Таблица 1.10 – Уязвимости, вызванные недостатками организации ТЗИ от НСД

Группа	Уязвимость	Степень опасности
1	2	3
Отсутствие ОРД	1. Отсутствие Инструкции по антивирусной защите в КАИС КРО	высокая
	2. Отсутствие Руководства администратора БД КАИС КРО, Руководства пользователя КАИС КРО	высокая
	3. Отсутствие Положения об организации режима безопасности помещений, где осуществляется работа с ПДн	высокая
Несоблюдение требований по защите информации		очень высокая
Неправильная организация контроля эффективности защиты информации		высокая

Проявление уязвимостей, вызванных недостатками организации технической защиты информации (ТЗИ) от НСД, возможны из-за:

- Недостаточного количества требуемых организационно-распорядительных документов в образовательных учреждениях;
- Недостаточного контроля эффективности мероприятий по защите информации в образовательных учреждениях и его структурных подразделениях;
- Незнания или игнорирования сотрудниками организационных требований при работе на объекте информатизации КАИСКРО.

1.4 Модель угроз безопасности веб-сайтов

К способам реализации угроз в КАИС КРО (обозначение «С» в указанных ниже таблицах 6.3 - 6.6) можно отнести следующие:

Физическое воздействие на технические средства КАИС КРО:

- Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов;
- Уничтожение, разрушение технического средства и линий связи;
- Нарушение электропитания технических средств;
- Изменение конфигурации технических средств;
- Несоблюдение организационных мероприятий по ЗИ.

Воздействие на каналы доступа, образованных с использованием штатных средств ИСПДн и обеспечивающих:

- Несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн и недостатков механизмов разграничения доступа;
- Компрометация технологической (аутентификационной) информации с использованием штатных средств ИСПДн;
- Нарушение адресности и своевременности информационного обмена;
- Сбои и отказы программно-технических компонентов КАИС КРО.

Обход СЗИ:

- Изменение настроек программных средств СЗИ;
- Перехват и вскрытие паролей;
- Изменение состава, используемого ПО и внедрение нештатного ПО.

Использование уязвимостей протоколов сетевого взаимодействия и каналов передачи данных:

- Перехват информации;
- Модификация передаваемых данных;
- Перегрузка ресурсов (отказ в обслуживании);
- Внедрение вредоносных программ;
- Удаленный несанкционированный доступ в систему.

Инфицирование программной среды:

- Передача управления на оригинальный загрузочный диск;
- Действия пользователя;

- Самостоятельная передача и запуск кода.

Угрозы НСД в КАИС КРО с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) персональных данных, и включают в себя:

– угрозы доступа (проникновения) в операционную среду с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

– угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

– угрозы внедрения вредоносных программ (программно-математического воздействия);

– угрозы, реализуемые при использовании протоколов межсетевого взаимодействия.

Используемый алгоритм описания угроз безопасности, включая правила отнесения угрозы безопасности к актуальной, определен в методическом документе ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Кроме того, в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных [4] определение типа угроз безопасности персональных данных, актуальных для информационной, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

Для нужд настоящей Частной модели угроз безопасности персональным данным КАИС КРО экспертами разработан оригинальный подход для получения оценок уровня вреда, наносимого субъектам персональных данных, и определения типов угроз безопасности персональных данных, актуальных для КАИС КРО.

Во втором столбце указан коэффициент реализуемости угрозы (Y), для вычисления которого используется числовой коэффициент вероятности реализации угрозы ($Y2$) и значение исходного уровня защищенности ($Y1$).

Под вероятностью реализации угрозы понимается показатель, характеризующий, насколько вероятным событием является реализация конкретной угрозы безопасности персональным данным для КАИС КРО в складывающихся условиях обстановки. Используются четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы;
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности персональных данных недостаточны;
- высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности персональных данных не приняты.

Каждой градации вероятности реализации угрозы поставлен в соответствие числовой коэффициент $Y2$, а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

Коэффициент реализуемости определяется соотношением $Y = (Y1 + Y2)/20$, где $Y1$ – исходный уровень защищенности КАИС КРО (рассчитан в пункте 3.1 настоящего документа и равен 10 (низкий уровень защищенности), $Y2$ – частота реализации угрозы).

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 < Y \leq 0{,}3$, то возможность реализации угрозы признается низкой;

– если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается средней;

– если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы высокая;

– если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

В третьем столбце оценивается значение вреда, наносимого субъектам персональных данных. В соответствии со статьёй 2 Федерального закона РФ от 27.07.06 № 152-ФЗ «О персональных данных», оценка вреда, который может быть причинён субъектам ПДн, производится в отношении прав и свобод человека и гражданина (субъекта ПДн), в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

При оценке вреда для субъектов ПДн на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель вреда. Этот показатель имеет четыре значения:

- отсутствие вреда – нарушение заданных характеристик безопасности ПДн не приводит к негативным последствиям для субъектов ПДн;
- не значительный вред – нарушение заданных характеристик безопасности ПДн может привести к незначительным негативным последствиям для субъектов ПДн;
- вред – нарушение заданных характеристик безопасности ПДн может привести к негативным последствиям для субъектов ПДн;

- значительный вред – нарушение заданных характеристик безопасности ПДн может привести к значительным негативным последствиям для субъектов ПДн.

В следующем столбце сводных таблиц оценивается опасность каждой угрозы. Вербальный показатель опасности угрозы имеет три значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Для определения значения опасности угрозы экспертами проведен анализ соотношения потенциального вреда для субъектов персональных данных и значения субъективной ценности персональных данных, содержащихся в КАИС КРО. Ценность ПДн для оператора ИСПДн установлена в условных единицах. Использованы следующие градации ценности персональных данных для оператора ИСПДн:

- уровень 4 (низкая) – менее 10 у.е.;
- уровень 3 (не значительная) – от 10 до 100 у.е.;
- уровень 2 (средняя) – от 100 до 1000 у.е.;
- уровень 1 (высокая) – свыше 1000 у.е.

Правило определения значения опасности угрозы приведено в таблице 1.11.

Таблица 1.11 - Правила определения опасности угрозы

Вред	Субъективная ценность			
	Низкая	Не значительная	Средняя	Высокая
1	2	3	4	5
Отсутствие вреда	низкая	низкая	низкая	низкая

Не значительный вред	низкая	низкая	средняя	средняя
Вред	средняя	средняя	средняя	высокая
Значительный вред	высокая	высокая	высокая	высокая

Определенный экспертами уровень ценности персональных данных, содержащихся в КАИС КРО, имеет значение уровень 1 (значительная ценность).

В последнем столбце сводных таблиц показана актуальность каждой угрозы. Выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным, осуществляется в соответствии с правилами, приведенными в таблице 1.12.

Таблица 1.12 - Правила отнесения угрозы безопасности к актуальной

Возможность реализации	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
1	2	3	4
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к информации связаны с доступом:

– к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) компьютерной техники КАИС КРО, с возможность перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;

– в операционную среду, то есть среду функционирования локальной операционной системы отдельного технического средства КАИС КРО, с возможностью выполнения НСД путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

– в среду функционирования прикладных программ (например, к системе управления базами данных);

– непосредственно к информации пользователя (к файлам, текстовой информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к КАИС КРО или, по крайней мере, к средствам ввода информации в КАИС КРО. Их можно объединить по условиям реализации в три группы.

Первая группа включает в себя угрозы, реализуемые в ходе загрузки операционной системы. Эти угрозы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения BIOS, перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду сетевых узлов КАИС КРО. Чаще всего, такие угрозы реализуются с использованием отчуждаемых носителей информации, в условиях отсутствия запрета загрузки с внешних носителей информации, или связаны с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении.

Проведенное обследование КАИС КРО показало, что пользователям КАИС КРО образовательное учреждение не запрещена загрузка операционной среды с внешних носителей. Поэтому объективные предпосылки для осуществления угроз, реализуемых в ходе загрузки операционной системы для рабочих станций пользователей, существуют. С учетом слабой мотивации пользователей на совершение подобных действий и их не высокой технической оснащенности вероятность реализации угрозы признается низкой.

Загрузка операционной среды с внешних носителей на серверах КАИС КРО разрешена только системному администратору. В связи с тем, что доступ в серверные помещения разрешен только ограниченному числу лиц, но объективные предпосылки для реализации угрозы существуют, вероятность реализации угрозы признается низкой.

Вторая группа – угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем. Эти угрозы, как правило, направлены на выполнение непосредственно НСД к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или какой-либо прикладной программы общего пользования, так и специально созданными для выполнения НСД программами в условиях отсутствия СЗИ от НСД и настройки операционных систем компьютерной техники КАИС КРО, например:

– программами просмотра и модификации реестра;

– специальными программами просмотра и копирования записей в базах данных;

– программами поддержки возможностей реконфигурации программной среды (настройки операционной среды и прикладного программного обеспечения в интересах нарушителя).

Третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз — это угрозы внедрения вредоносных программ.

1.5 Анализ атак веб-сайтов и выбор средств защиты персональных на основе анализа их защищенности

Вопрос выбора средств защиты является достаточно актуальным, и, конечно, много кто пытался найти на него наиболее подходящий ответ. Предлагаемые решения основаны на самых разных принципах и используют самые разные алгоритмы для достижения цели. Однако используемый подход может приводить и к тому, что алгоритм выбора потеряет свою универсальность и гибкость, что, конечно, не идёт ему на пользу в ключе удобства использования и применимости к конкретной системе защиты. Ниже

приведены некоторые способы решения проблемы выбора средств защиты информации:

1. Использование компьютерных игр для определения методов и средств защиты информации. Способ, предложенный А.Ф. Белым, является по своей сути имитационном моделированием тех процессов, которые происходят в реальном мире при проектировании и создании реальных систем защиты ПДн [15]. Компьютерная игра для выбора методов и средств защиты информации представляет собой комплекс программ, предназначенный для моделирования в реальном масштабе времени возможных действий нарушителя на уязвимости система защиты ПДн, адекватных мер защиты информации, процессов функционирования системы на заданном интервале времени и оценки эффективности выбранных вариантов игры.

Компьютерная игра служит для выработки рекомендаций по рациональным действиям и согласованному выбору средств защиты при разработке компонентов системы и средств защиты информации в условиях наличия неопределенности действий нарушителя.

Подобные технологии имитации реальных процессов применяются и при защите от сетевых атак – так называемая технология honeypot, то есть в буквальном переводе с английского – горшочек с мёдом. Суть технологии заключается в первую очередь, в дублировании системы, на которую может быть осуществлена атака хакеров, и в мониторинге с последующей записью в журнал всех действий хакеров при совершении атаки на систему. Дублирование может осуществляться как посредством виртуализации, так и за счёт использования специализированного программного обеспечения, создающего иллюзию разветвлённой сетевой инфраструктуры для хакера. В дальнейшем чёткое понимание действий хакера, записанное в журнал, может быть применено для создания реальных систем защиты.

Возвращаясь к компьютерной игре, можно сказать, что большим плюсом такого способа является возможность наиболее полно рассмотреть все возможные уязвимости реализуемой системы защиты, применить необходимые

средства и методы для их нивелирования, и, таким способом добиться наибольшей защищённости системы защиты ПДн. Разумеется, реализовать такой способ можно лишь при сотрудничестве с огромным количеством экспертов в самых разных областях для наиболее полного раскрытия всевозможных характеристик, уязвимостей, возможностей и так далее.

Однако при условии создания подобной компьютерной игры с огромной базой знаний по всевозможным средствам и методам защиты, уязвимостям, способами атак и способам использования уязвимостей, можно получить уникальный во всех смыслах слова инструмент, позволяющий с большой точностью предсказать всевозможные варианты поведения нарушителя, а значит, и предложить наиболее подходящие способы защиты от его неправомерных действий. Имея такой инструмент, можно разработать универсальные модели систем защиты для различных сфер деятельности, будь то банковская сфера, малый бизнес, медицина или любая другая.

К явным же минусам такого способа можно отнести его масштабы, денежные средства, которые придётся потратить на разработку подобного программного комплекса, трудозатраты, ну, и конечно затраты времени.

2. Использование способа, предложенного В.П. Ивановым и В.Ю. Фёдоровым, позволяющего сделать выбор СЗИ на основании оценки стойкости технических средств от злоумышленного изучения [16].

Тот факт, что системам защиты информации от НСД присуща неопределенность, предполагает положить в основу выбора технических средств защиты информации от НСД показатели эффективности вероятностно-временной группы:

- время безопасного функционирования защищаемой системы;
- время безопасного функционирования защищаемых систем с эффективностью защиты информации от НСД не ниже заданной;
- экономическая эффективность функционирования системы защиты
- информации от НСД.

Выводы по разделу 1

Все приведённые способы, к сожалению, не являются идеальными решениями проблемы выбора СЗИ, но использование их всех или некоторых из них для создания одного мощного алгоритма выбора может стать действенным способом для решения поставленной задачи по выбору средств защиты информации.

Рассмотрев имеющиеся способы решения проблемы выбора средств защиты информации, можно выдвинуть несколько тезисов:

- алгоритм должен быть доступным, чтобы реализовать его даже на бумаге, без использования электронных средств и без специальных знаний;
- алгоритм должен быть гибким;
- алгоритм должен быть масштабируемым;
- алгоритм должен быть объективным;
- алгоритм должен предусматривать интегрируемость.

2 РАЗРАБОТКА ПРОЕКТНЫХ РЕШЕНИЙ ПО СОЗДАНИЮ ПК КОНТРОЛЯ ЗАЩИЩЕННОСТИ ВЕБ-САЙТОВ

2.1 Общее положение о разработке алгоритма контроля защищенности веб-сайтов

Атака MAC-flooding относится к классу разведывательных атак. Этот вид атаки может использоваться также в качестве DoS-атаки. Атакующая машина забивает переключатель (switch) огромным числом кадров с неверными MAC-адресами отправителя. Переключатели имеют ограниченную память для таблицы переадресации (MAC-порт) и при такой атаке таблица будет заполнена некорректными MAC-адресами, пришедшими от машины-атакера. При поступлении легального трафика из-за отсутствия соответствующих записей в таблице переадресации пакеты будут направляться на все выходы переключателя. В результате атакер, взломавший машину, которая реализует данную атаку, получит большое количество ценной для него информации. Кроме того, это может вызвать перегрузку каналов и самого переключателя (рисунок 2.1).

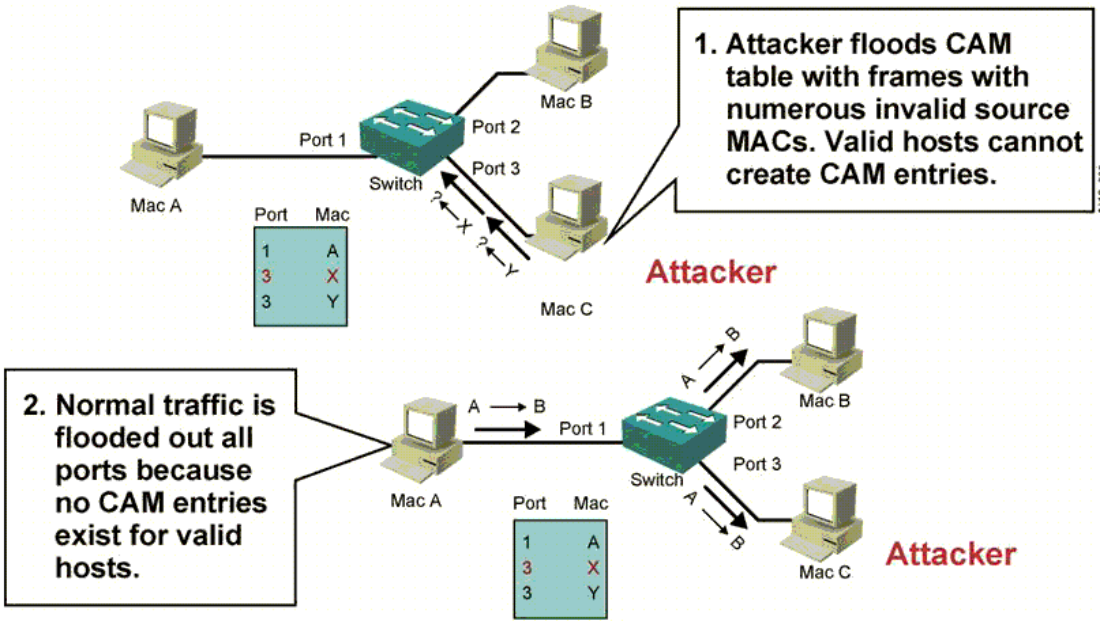

Рисунок 2.1 - Схема атаки MAC-flooding

Следует учитывать, что характер атак становится все более изощренным. Хакеры объединяются в клубы, издают журналы и продают хакерские CD. Сегодня крайне актуальным становится кооперирование их потенциальных

жертв. Для профессиональных DDoS атак могут использоваться машины, взломанные ранее (зомби). Большие группы таких машин иногда называются армиями.

Обычно наибольшее внимание привлекают атаки из области вне локальной сети (SQL или XSS-injection). Реально несравненно большую угрозу представляют визиты сотрудников в социальные сети (Facebook, Twitter и т.д.), e-mail phishing или drive-by download (так называетмые приглашенные атаки), а также атаки инсайдеров (сетевые объекты, работающие в области, защищенной сетевым экраном). В случае посещения вредоносного сайта киберпреступники могут просканировать машину жертвы на предмет наличия известных уязвимостей. Под инсайдером подразумеваются не только сотрудники, работающие в локальной сети, но также скомпрометированные машины LAN (например, посредством USB-флэшей или любых других переносимых носителей или laptop'ов). Классическим примером инсайдерской атаки является утечка данных госдепартаметна США, опубликованных на сервере WikiLeaks.

2.2 Алгоритмы тестирования веб-сайтов на уязвимости

В этом сценарии проводятся тесты DoS-атак на основе сообщений IPv6 ND, таких как фальшивая реклама маршрутизатора, фальшивые ответы на DAD и запросы на выявление фальшивых соседей. В этом исследовании будут проверены атаки Smurf или ICMP разработанным пакетами. Инструменты для использования в этом сценарии включают *ra6, rd6* и *fake_router26*. Варианты в этом сценарии включают нижеописанные сценарии.

DoS через переадресацию ICMPv6.

Тест-сериал, предназначенный для этого исследования, состоит из двух маршрутизаторов, одного брандмауэра, одного переключателя, один веб-сервера, одного DNS-сервера и DHCP-сервера, двух клиентов, одной мониторной машины и одного нападающего.

Шлюз в сети подключается ко второму маршрутизатора, который затем подключается к веб-серверу. Второй маршрутизатор и веб эмулируют внешнюю сеть, такую как Интернет.

Сканирование выполним следующими командами

Для Cisco первые два случая изображенном на рисунке 2.2.

```
#  alive6 eth0 fdd2:8a70:0f46:1::0-ff
```

Рисунок 2.2 – Команды для Cisco для первого и второго случая

Для третьего и четвертого случая используются команды, изображенные на рисунке 2.3.

```
#  scan6 -d fdd2:8a70:0f46:1::0-ff -p all -v
```

Рисунок 2.3 – Команды для Cisco для третьего и четвертого случая

В результате из четырех сканированных выполненных 3 были в состоянии идентифицировать все 4 устройства в локальной сети.

Однако, когда все брандмауэры выключались, оба инструмента идентифицировали все устройства. Использование *alive6* сканирования занимает примерно 24 минут для идентификации всех устройств и 25 минут для завершения сканирования.

Для проверки результатов scan6 использовался с различными параметрами (рисунок 2.4 и 2.5).

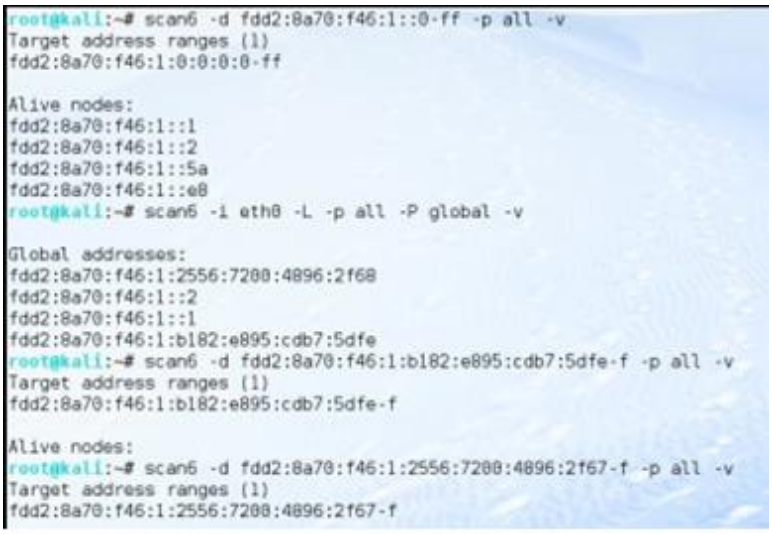

Рисунок 2.4 – Результаты сканирования

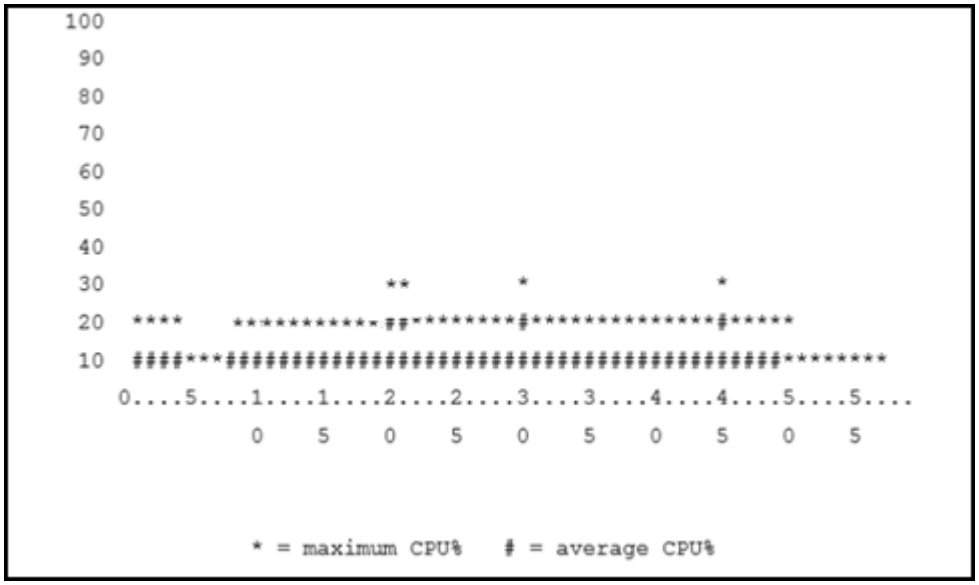

Рисунок 2.5 – Загрузка ЦП маршрутизатора Cisco во время атаки

В этом тесте компьютер нападающего пытается настроить атаку MITM путем затопления рекламы фальшивых роутеров в локальной сети. Атака MITM также проверяется, когда жертва обратилась к веб-серверу извне. Этот сценарий будет проверено двумя различными способами, которые включают использование фальшивых рекламных роутеров и сообщений с переадресацией ICMP.

ПК-атакующий настраивается в режиме переадресации, чтобы пересылать все полученные пакеты на реальный маршрутизатор и не нарушать связи в сети.

Для настройки злоумышленника в режиме переадресации использовались следующие команды для Cisco:

1. redir6 eth0 fe80 :: 31f7: a831: a2b3: 5a08 fdd2: 8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff: fef7: 5949 fe80 :: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8;

2. redir6 eth0 fe80 :: 21a: a0ff: fea4: 4ae9 fdd2: 8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff: fef7: 5949 fe80 :: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8.

До и после каждого теста на клиентских компьютерах запускаются *ping* и *traceroute*, чтобы проверить путь пакетов. Кроме того, клиенты будут пытаться получить доступ к веб-серверу после того, как атака MITM работает.

Когда началась первая атака, оба клиенты получили рекламные сообщения маршрутизатора и добавили IP-адрес к своим сетевым интерфейсам. Windows 7 немедленно начал использовать новый маршрутизатор, и на него было отправлено весь трафик. Результаты с Ubuntu 22.09 были прерывистые. В большинстве случаев Ubuntu направил все пакеты на маршрутизатор. *Ping* и *traceroute* использовались для проверки того, что пакеты были отправлены через злонамеренный ПК. Клиент отправлял пакеты атакующим и отправляя пакеты на маршрутизатор, и в течение последних тестов он только отправил трафик на маршрутизатор. Трафик проходил только от одного клиента к атакующему к маршрутизатору, а непосредственно возвращался с маршрутизатора непосредственно клиентам.

Испытания доступа к сайту показало, что атака не только добавляет новую IP-адрес, но и изменяет параметры сети в клиентах. Поскольку клиенты предпочли RA от злоумышленника, они не обращали внимания на DNS, предоставленный DHCP, поэтому домен *www.ipv6tb.edu,* указывающий на веб-сервер, не может быть решен. При попытке получить доступ к веб-серверу, используя его IP-адрес, вместо имени домена, работал, а атакующий смог зафиксировать некоторые HTTP-пакеты. В частности, TCP + SYN-пакеты, отправленные в начале соединения.

Наконец, перенаправление пакетов ICMP, отправленных с помощью *redir6*. Не повлияло на таблицы маршрутизации клиентов или их маршруты. Пакеты были получены, но не вставили новый путь к таблицам маршрутизации клиентов (рисунок 2.6 и 2.7).

```
C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::1
  2    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46::2
  3    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>ping fdd2:8a70:f46:2::2

Pinging fdd2:8a70:f46:2::2 with 32 bytes of data:
Reply from fdd2:8a70:f46:2::2: time=1ms
Reply from fdd2:8a70:f46:2::2: time=1ms
Reply from fdd2:8a70:f46:2::2: time=1ms
Reply from fdd2:8a70:f46:2::2: time=1ms

Ping statistics for fdd2:8a70:f46:2::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     1 ms     1 ms  fdd2:8a70:f46:1::1
  3     1 ms     1 ms     1 ms  fdd2:8a70:f46::2
  4     1 ms     1 ms     1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>tracert www.ipv6tb.edu
Unable to resolve target system name www.ipv6tb.edu.

C:\Users\CCENT>
```

Рисунок 2.6 – Результаты на ПК Windows во время теста Cisco

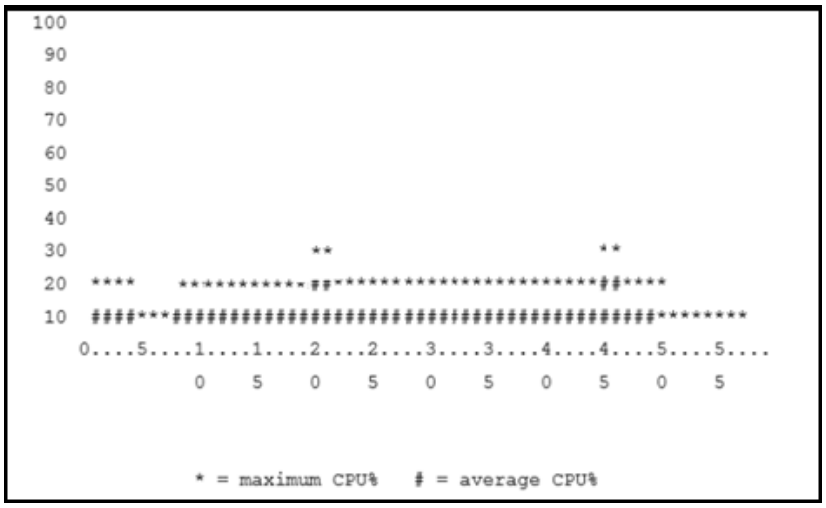

Рисунок 2.7 – Загрузка ЦП маршрутизатора Cisco во время атаки

Этот сценарий свидетельствует о том, что атаки MITM с использованием фальшивых рекламных роутеров в IPv6 не столь эффективны, как ARP в IPv4. Несмотря на то, что *parasite6* выполняет подделку соседей IPv6 (подобно IPv4 ARP) на IPv6, результаты были непоследовательными, и сама сеть стала нестабильной. Использование фальшивых рекламных роутеров успешно вводит фальшивый маршрут в Windows и захватывает трафик, который направляется изнутри наружу. Путь, который путешествует по-другому, не был направлен на злонамеренный ПК. Это показывает, что злоумышленник выполнял "половину"

MITM, поскольку он мог только захватывать исходящий трафик. Это создает прецедент для последующего сценария, в котором одинаковое тестирование будет выполняться с помощью брандмауэра как шлюза.

Процедура замены сообщение RA.

В этом тесте компьютер нападающего пытается настроить атаку MITM путем затопления рекламы фальшивых роутеров в локальной сети. Эти объявления объявляют атакующего качестве маршрутизатора и прямой трафик в сети к нему. В этом сценарии DCHP используется для настройки маршрутизатора, чтобы рекламировать его в своих пакетах RA.

Нападающий ПК настраивается в режиме переадресации для пересылки всех пакетов в настоящий маршрутизатор и не нарушают связи в сети. В таблице 4 приведены подробности устройств, подключенных к локальной сети в этом сценарии.

Для настройки злоумышленника в режиме переадресации использовались команды для Cisco изображенные на рисунке 2.8.

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:f9ff:fef7:5949 dev eth0
#  fake_router26 -A fdd2:8a70:0f46:1::/64 -a 30 eth0
```

Рисунок 2.8 – Команды для Cisco

ICMP-сообщение перенаправления не проверены, поскольку они не дали никаких результатов в предыдущих сценариях. До и после каждого теста на клиентских компьютерах запускаются *ping* и *traceroute*, чтобы проверить путь пакетов. Кроме того, клиенты пытаются получить доступ к веб-серверу после того, как атака MITM работает.

Перед началом атаки клиенты получили адрес IPv6 и могли без проблем пользоваться веб-сервером, используя его доменное имя. После запуска атаки компьютер Ubuntu изменил маршрут по умолчанию после получения фальшивых пакетов рекламы маршрутизатора и зарегистрировал фальшивый маршрутизатор в своей таблице маршрутизации. Во всех тестах, выполненных в этом сценарии, атака MITM работала на клиенте Ubuntu. Подобным образом, ПК Windows также стал посылать трафик злоумышленнику после того, как

атака была разочарована. Она зарегистрировала атакующего качестве маршрутизатора по умолчанию в своей таблице маршрутизации, и к нему был отправлен весь трафик. Команда traceroute показала, что сначала трафик направляется нападающему, а затем маршрутизатору.

Потерянный трафик на злоумышленника и монитора показывает, что злоумышленник может видеть только исходящие сообщения, отправленные жертвой. Злоумышленник не получает никакого ответа, которая возвращается. Кроме того, у клиента Windows, который потерял связь, не удалось найти DNS для решения имени веб и не могло получить доступ к нему. Фактический адрес IPv6 веб использовалась вместо того, чтобы зайти на сервер (рисунок 2.9 и 2.10).

```
C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        1 ms  fdd2:8a70:f46:1::1
  3     *        *        *     Request timed out.
  4     1 ms    <1 ms    <1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        *     fdd2:8a70:f46:1::1
  3     *       <1 ms    <1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>
```

Рисунок 2.9 – Traceroute от клиента Windows веб-сервера во время атаки MITM для Cisco

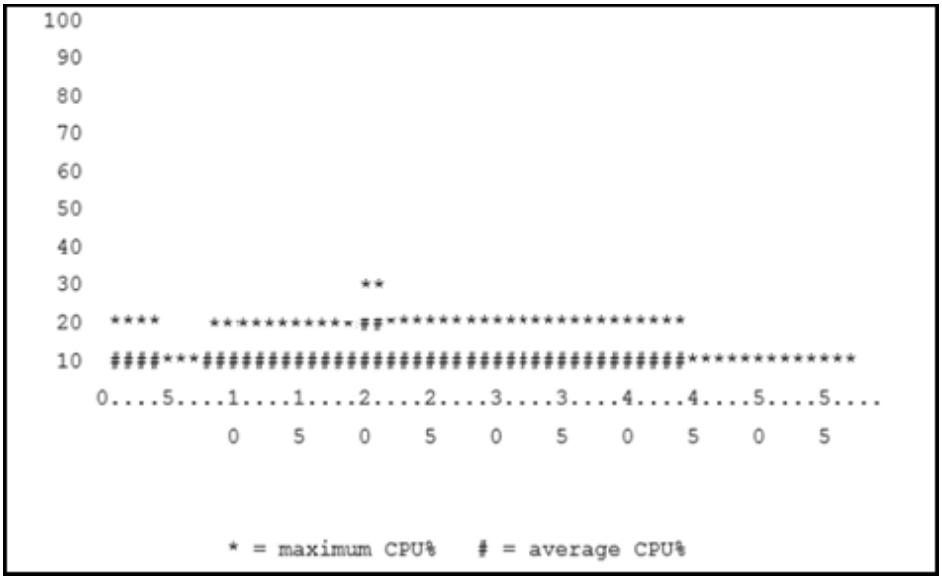

Рисунок 2.10 – Загрузка ЦП маршрутизатора Cisco во время атаки

Как и результаты, полученные в предыдущем сценарии, эти результаты показывают, что злоумышленник может захватывать трафик, однако он не завершает общую атаку MITM, поскольку не может прочитать входящие пакеты. Вероятно, что маршрутизатор определяет назначение входящих пакетов в таблице соседей и направляет пакет прямо к клиенту. Это невозможно подтвердить в захваченных пакетах. Фактически, некоторые сообщения перенаправления, сделанные с помощью Wireshark, позволяют предположить, что злоумышленник может не находиться в центре коммуникации, так как атака MITM должна быть. Если первая гипотеза истинна, следует иметь брандмауэр как шлюз по умолчанию разорвать соединение с клиентом и отказаться от атаки MITM.ASA 5510 – это стабильный брандмауэр и открывает связь с внешней средой для клиента, его запускает. В случае MITM, если это действительно "наполовину" атаки MITM, брандмауэр должен заблокировать соединение, поскольку все ответы предназначены клиенту, но злоумышленник запустил соединения.

Процедура подмены сообщения NA.

В этом тесте компьютер нападающего пытается настроить атаку MITM путем затопления рекламы фальшивых роутеров в локальной сети. В этом случае, учитывая, что версия IOS в используемом брандмауестри не поддерживает конфигурацию DHCP на пакетах рекламы маршрутизатора, SLAAC будет использоваться без DNS. Тесты на сайт внешне выполняются с помощью адреса IPv6 веб-сервера. Этот сценарий будет проверен с помощью фальшивых рекламных роутеров.

ПК-атакующий настраивается в режиме переадресации, чтобы пересылать все полученные пакеты на реальный маршрутизатор и не нарушать связи в сети.

Для настройки злоумышленника в режиме переадресации использовались команды для Cisco изображенные на рисунке 2.11.

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:c6ff:fefa:470f dev eth0
#  fake_router26 -A fdd2:8a70:0f46:1::/64 -a 30 eth0
```

Рисунок 2.11 – Команды для Cisco

ICMP-сообщения переадресации не проверяются, поскольку они не дали никакого результата в предыдущем сценарии. До и после каждого теста на клиентских компьютерах запускаются *ping* и *traceroute*, чтобы проверить путь пакетов. Кроме того, клиенты пытаются получить доступ к веб-серверу после того, как атака MITM работает.

Выводы к разделу 2

Этот сценарий давал разные результаты для каждого клиента, как это случилось в предыдущем сценарии. Как и в предыдущем сценарии, клиент Windows начал использовать атакующего как шлюз по умолчанию, как только началась атака. С другой стороны, Ubuntu получил сообщение PA, создал запись в своей таблице маршрутизации, но продолжал использовать маршрутизатор как шлюз по умолчанию. *Ping* и *traceroute* были успешными в обоих случаях.

3 ТЕСТИРОВАНИЕ И ОЦЕНКА ЭФФЕКТИВНОСТИ РАЗРАБОТАННОГО ПРОГРАММНОГО КОМПЛЕКСА

3.1 Анализ эффективности мер обеспечения безопасности веб-сайтов с помощью разработанного программного комплекса

Рассмотрим результаты тестирования, проведенного в подглаве 2.2.

Таблица 3.1 – Результаты проведенного тестирования

Атаки	Внутренние	Внешние	Firewall	Скрытые	Разведка	Наличие	
						Уязвимости	Средств предупреждение
1	2	3	4	5	6	7	8
Разведка в IPv6 сети	x	x	x	x	x	+	-
Smurf атака	x	x				-	-
Стек заголовков расширение	x		x	x		+	- / +
Подмена сообщение RA	x		x	x		-	-
Подмена сообщение NA	x		x			-	-
Подмена DHCPv6 сервера	x		x	x	x	-	+
Вторжение в тоннель	x	x		x	x	+	- / +

Значительная часть атак приводит или к отказу в обслуживании, или к перехвату пользовательского трафика, и в большинстве случаев жертвами становятся конечные устройства. Более опасны атаки с использованием заголовков расширения, в результате которых может произойти отказ в обслуживании на уровне маршрутизаторов, или утечка информации.

Оценка определенных уязвимостей рассчитывается по основной группой метрик, в результате дают числовое значение основной оценки CVSS, оценки воздействия и оценки уязвимости. Как результат, определены оценку уровня

риска уязвимости с учетом критичности устройства. Результаты представлены в таблице 3.2.

Таблица 3.2 – Оценки уязвимостей

Атаки	Основная оценка CVSS	Оценка воздействия	Оценка уязвимости	Оценка уровня риска уязвимости
1	2	3	4	5
Разведка в IPv6 сети	0	0	1.2	C
Smurf атака	5.3	2.1	10.7	C
Стек заголовков расширения	4.0	2.6	10.0	A
Подмена сообщение RA	7. 2	6. 3	6.5	B
Подмена сообщение NA	2.1	2. 8	3. 1	C
Подмена DHCPv6 сервера	7.5	6.9	6.8	A
Вторжение в тоннель	3.0	2.0	10.9	B

По результатам оценки уязвимости, оборудование Cisco устраняет только уязвимости уровня A, остается возможной одна атака уровня B (подмена сообщение RA) и три атак и уровня C. Это означает, что данный сегмент сети имеет средний уровень защищенности.

3.2 Функциональная эффективность программы

Проанализируем функциональную эффективность программного комплекса Windows прежде всего направил все свои пакеты атакующему. Ubuntu продолжал использовать маршрутизатор как шлюз по умолчанию.

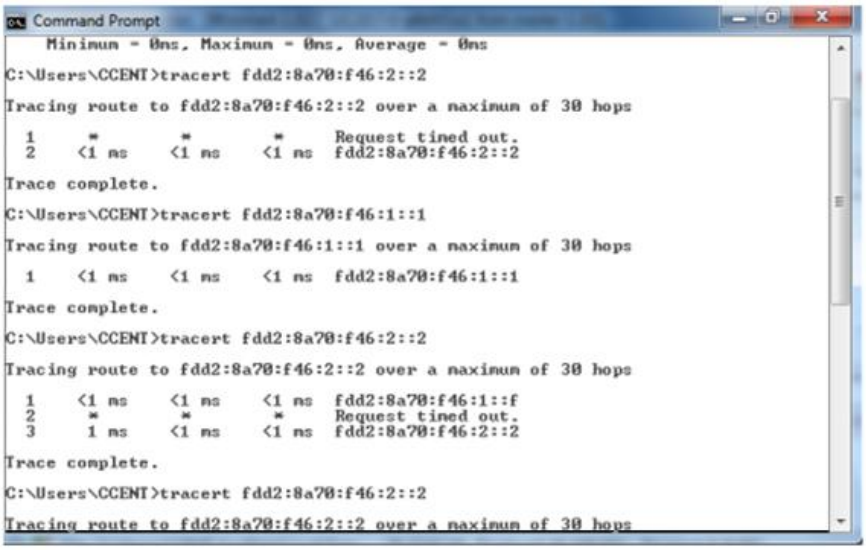

Рисунок 3.1 – Traceroute от клиента Windows при MITM за брандмауэром для Cisco

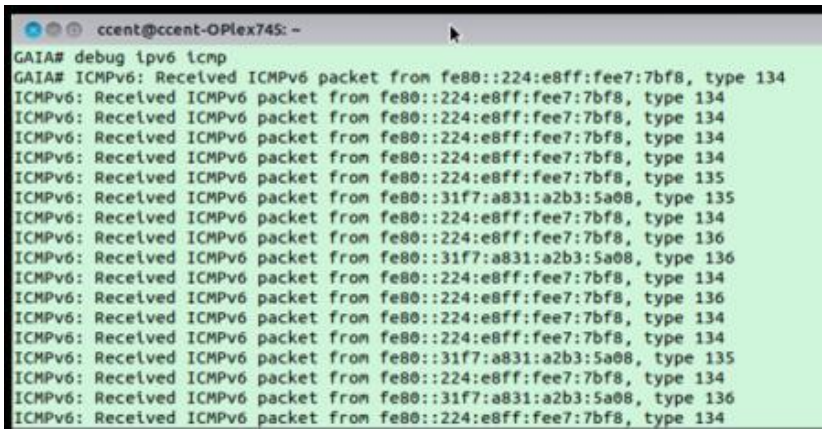

Рисунок 3.2 – Сообщение ICMPv6, снятые на брандмауэре ASA вовремя MITM за брандмауэром для Cisco

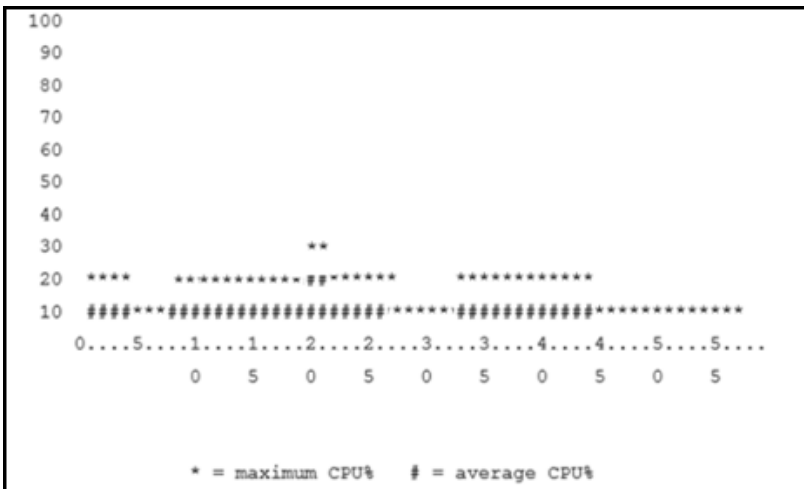

Рисунок 3.3 – Загрузка ЦП маршрутизатора Cisco во время атаки

Этот сценарий показал, как работает атака MITM с *fake_router26*. В начале этого сценария и на основании предварительных выводов ожидаемый результат – брандмауэр, блокирующий ответа от эхо извне, поскольку адресат был другим хостом от той, которая открыла соединения. Тестирование показало, что брандмауэр позволяет выполнять запросы и ответы с помощью эхо в этом сценарии. Этот результат вызвал вопрос об операции MITM.

Дальнейший анализ переданных клиентом и злоумышленником, показывает, что злоумышленник не пересылает полученные пакеты, а вместо этого отвечает пострадавшему с помощью ICMP-сообщение с перенаправлением, что указывает на маршрутизатор.

Выводы по разделу 3

Значительная часть атак приводит или к отказу в обслуживании, или к перехвату пользовательского трафика, и в большинстве случаев жертвами становятся конечные устройства. Более опасны атаки с использованием заголовков расширения, в результате которых может произойти отказ в обслуживании на уровне маршрутизаторов, или утечка информации.

Оценка определенных уязвимостей рассчитывается по основной группой метрик, в результате дают числовое значение основной оценки CVSS, оценки воздействия и оценки уязвимости. Как результат, определены оценку уровня риска уязвимости с учетом критичности устройства.

ЗАКЛЮЧЕНИЕ

Сканеры — это первый инструмент, используемый злоумышленником для выявления их жертв и определения возможных атак на запуск. IPv6 предлагает некоторую защиту от этих инструментов, хотя это не пуленепробиваемое. Большой размер адресов IPv6, доступных для интерфейсов, затрудняет использование сканерами традиционного способа тестирования всех IP-адресов, отправляют ICMP-пакеты. В первом сценарии, использует alive6, этот процесс принял так долго, что использование его в реальной сети с префиксом /64 будет непрактичным.

Использование созданного пакета эхо-пакетов ICMPv6, а также простых пакетов echo ICMPv6, направленных на багатоадрес-адреса, является лучшим способом поиска адресов IPv6, используемых. Преимущество разработанных пакетов заключается в том, что они также могут найти хосты Windows. Во время сканеров один из результатов заключался в том, что системы Windows не реагируют на многоканальные ехоподибни пакеты ICMPv6.

Однако созданные пакеты создают ответ из систем Windows, которые могут использоваться для сканирования сети. Наконец, время, необходимое для сканирования сети, используя многоадресные пакеты, является минимальным.

Тестирование сообщений о рекламе маршрутизации в атаках MITM показывает, что способ, которым операционные системы обрабатывают эти пакеты, могут создавать уязвимость системы безопасности. В этом случае трудно назначить ответственность, поскольку стандарт не указывает, каким образом следует обрабатывать эти пакеты, таким образом операционные системы имеют свободу реализации собственных решений. Как было показано, Windows имеет некоторые проблемы с обработкой этих пакетов.

Исходя из результатов, делается вывод, что способ обработки сообщений PA делает разницу между безопасной или опасной средой. Возможно, что полностью совместима сеть IPv6, которая использует IPsec, преодолеет эти проблемы, однако сейчас ОС должны найти надежный механизм для проверки сообщений PA. Эти решения могут предусматривать дополнительные пакеты,

отправляемые по сети, проверка MAC-адреса, установление приоритетов сети на основе времени или даже ручная проверка. Все эти методы также приносят новые проблемы, которые могут сделать их непрактичным.

Несмотря на то, что атаки MITM в IPv6 все еще возможны, их настроить немного сложнее, чем это делается в сети IPv4, когда узлы IPv6 используют адреса локальной линии. Однако важно отметить, что полная реализация IPsec в IPv6 позволит преодолеть эту проблему, по крайней мере теоретически, через ее процесс аутентификации. Атака MITM не может быть успешной в подключении IPsec, или, по крайней мере, это будет сложнее для реализации.

Использование инструмента fake_router26 показало, что атака MITM частично реализована. Фактически, эта атака превращает атакующую машину на сниффер, который фиксирует весь трафик, поступающий от жертв, но не может зафиксировать трафик на них. Это происходит потому, что, когда жертва устанавливает связь с назначением, общение происходит только между ними, а атакующий не может нюхнуть трафик в коммутируемой сети. Чтобы зафиксировать весь трафик, атакующий должен или рекламировать другую сеть, так и выступать в качестве шлюза или выдать себя за маршрутизатор и выполнять роль прокси-сервера.

Испытания показали, что атака MITM также может стать атакой "Отказ в обслуживании", поскольку это влияет на конфигурацию DNS сети с DHCP, также заставляет обычных пользователей доступа к Интернету. Регулярные пользователи будут пытаться получить доступ к веб-сайту или службы и не сможет из-за атаки. Если реализовано среду, вроде этого отчета, другие конфигурации могут быть проверены, чтобы оценить, они дают сходные результаты. Основной проблемой использования рекламных сообщений маршрутизатора является то, что жертва перестает слушать DHCP-сервер, и поэтому не получает IP-адрес. Это может привести к срыву работы корпоративной сети, которая становится атакой отказа в обслуживании.

Имеющиеся отказа в предоставлении услуг все еще составляют проблему в IPv6. Способ, которым операционные системы обрабатывают пакеты RA, не

является проблемой только для атак MITM, а также для атак отказа в обслуживании. Операционные системы, которые обрабатывают все сообщения PA без всякой валидации или ограничения, уязвимые к исчерпанию ресурсов, использующих наводнения сообщений PA. Большое количество этих сообщений заставляет жертвы использовать все свои ресурсы при их обработке и в конечном счете сбои. Несмотря на то, что различные операционные системы отличаются от этих сообщений, они, по крайней мере, должны ограничивать ресурсы, доступные для этой задачи, или устанавливать ограничения на количество использованных ресурсов. Системы Windows достигли некоторых успехов в этом поле, но это все еще остается позади.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. ГОСТ 19.701-90. Единая система программной документации. Схемы алгоритмов, программ, данных и систем.

Научная и методическая литература

2. Aura T. Cryptographically generated addresses (CGA). – 2005.

3. Bagnulo M. Efficient security for IPv6 multihoming / M. Bagnulo, A. García-Martínez, A. Azcorra // ACM SIGCOMM Computer Communication Review. – 2005. – Т. 35. – №. 2. – С. 61-68.

4. Bos J.W. Analysis and optimization of cryptographically generated addresses / J.W. Bos, O. Özen, J.P. Hubaux // Information. – 2009

5. Bagnulo M. Cryptographically Generated Addresses (CGA) Extension Field Format / M. Bagnulo, J. Arkko. – 2006.

6. Bos J.W. Analysis Optimization of Cryptographically Generated Addresses / J.W. Bos, O. Özen, J.P. Hubaux // In Proceedings of the 12th International Conference on Information Security (ISC). – Berlin. – Heidelberg. – 2009. – С. 17-32.

7. Arkko J. Secure neighbor discovery (SEND) / J. Arkko, Ed. Ericsson, J. Kempf. – 2005.

8. Combes J. M. et al. CGA as alternative security credentials with IKEv2: implementation and analysis // SAR-SSI'12: 7th Conference on Network Architectures and Information Systems Security. – 2012. – С. 53-59.

9. Bagnulo M. Hash-based addresses (HBA). – 2009.

10. Davies E. IPv6 transition / E. Davies, S. Krishnan, P. Savola // co-existence security considerations. – 2007.

11. McGann O. IPv6 Packet Filtering, a Master’s Thesis at Department of Electrical Engineering, National University of Ireland Maynooth, Supervised by David Malone. – 2005.

12. Krishnan S. Handling of Overlapping IPv6 Fragments. – December, 2009.

13. Deering S. E. Internet protocol, version 6 (IPv6) specification. – 1998.

14. Davies E. Recommendations for filtering icmpv6 messages in firewalls / E. Davies, J. Mohacsi. – May, 2007.

15. Gont F. Requirements for IPv6 Enterprise Firewalls / F. Gont, M. Ermini, W. Liu. – April, 2014.

16. Jankiewicz E. IPv6 Node Requirements / E. Jankiewicz, J. Loughney, T. Narten. – December 2011.

17. Loughney J. IPv6 node requirements. – 2006.

18. Korver B. The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX. – August, 2007. – p. 43.

19. Graveman R. et al. Using IPsec to Secure IPv6-in-IPv4 Tunnels / R. Graveman, M. Parthasarathy, P. Savola, H. Tschofenig. – May, 2007. – p. 23.

20. Devarapalli V. Mobile IPv6 operation with IKEv2 and the revised IPsec architecture / V. Devarapalli, F. Dupont. – 2007. – p. 26.

21. Frankel S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap / S. Frankel, S. Krishnan – February, 2011. – p. 63.

22. Bi J. SAVI Solution for DHCP. / J. Bi, J. Wu, G. Yao, F.Baker. – May, 2014. – p. 43.

23. McPherson D. Source Address Validation Improvement (SAVI) Threat Scope / D. McPherson, J. Halpern, F. Baker. – May, 2013. – p. 25.

24. Bagnulo M. SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI) / M. Bagnulo, A. Garcia-Martinez. – May, 2014. – p. 38.

25. Levy-Abegnoli E. IPv6 Router Advertisement Guard / E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi. – February, 2011. – p. 10.

26. Gont F. Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard). – February, 2014. – p. 13.

Электронные ресурсы

27. IPv6 First-Hop Security Configuration Guide, Cisco IOS Release 15S [Электронный ресурс:] – Режим доступа:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book .pdf.

28. Economou, N. Core Security. Microsoft Windows TCP IPv6 Denial of Service Vulnerability [Электронный ресурс:] – Режим доступа: http://blog. coresecurity.com/2014/03/25/ms14-006-microsoft-windows-tcp-ipv6-denial-of-service-vulnerability/#sthash.iBLIqqwp.dpuf

29. McDowell, M. US-CERT. Understanding Denial-of-Service Attacks [Электронный ресурс:] – Режим доступа: http://www.us-cert.gov/ncas/tips/ ST04-015

30. Microsoft Developer Network. IPv6 Addressing [Электронной ресурс:] – Режим доступа: http://msdn.microsoft.com/en-us/library/ aa917150.aspx

31. Narten, T., Nordmark, E., Simpson, W., & Soliman, H. Internet Engineering Task Force (IETF). RFC4861 Neighbor Discovery for IP version 6 (IPv6) [Электронный ресурс:] – Режим доступа: http://tools.ietf.org/html/rfc4861

ПРИЛОЖЕНИЕ А

Код программы:

```
unit IPParse;

interface

uses
  Windows, SysUtils, Classes, RTLConsts, Dialogs;

type
TIPInt      = Integer;
PIPItemList = ^TIPItemList;
TIPItemList = array of TIPInt;
TIPStr      = record
    A1, A2, A3, A4 : string[3];
  end;

TCNCallBack = procedure (Num: Byte; Prefix: string; Obj: Pointer);
TIPList = class(TStrings)
private
FCount      : Integer;
FLength     : Integer;
FUpdating   : Boolean;
FIPItemList :TIPItemList;
FOnChange   : TNotifyEvent;
FOnChanging :TNotifyEvent;
    _A1, _A2, _A3, _A4 : string;
functionIPIntToIPStr(Value: TIPInt): TIPStr;
functionIPStrToIPInt(Value: TIPStr): TIPInt;
functionIPIntToStr(Value: TIPInt): string;
functionStrToIPInt(Value: string): TIPInt;
procedureGrow;
procedureUpdateMem;
functionEnumChaptNums(Mask: string; CallBack: TCNCallBack; Prefix: string): Integer;
  protected
    procedure Changed; virtual;
    procedure Changing; virtual;
function Get(Index: Integer): string; override;
functionGetIPInt(Index: Integer): TIPInt;
functionGetIPStr(Index: Integer): TIPStr;
functionGetCount: Integer; override;
procedure Put(Index: Integer; const S: string); override;
procedurePutIPInt(Index: Integer; const S: TIPInt);
procedurePutIPStr(Index: Integer; const S: TIPStr);
procedureSetUpdateState(Updating: Boolean); override;
published
procedureClear; override;
procedure Delete(Index: Integer); override;
procedure Insert(Index: Integer; const S: string); override;
function Add(const S: string): Integer; override;
```

```
procedure Exchange(Index1, Index2: Integer); override;
functionProcessSingleMask(Mask: string): Integer;
functionParseMask(Mask: string): Integer;
  public
propertyAsIPInt[Index: Integer]: TIPInt read GetIPInt write PutIPInt;
propertyAsIPStr[Index: Integer]: TIPStr read GetIPStr write PutIPStr;
    property OnChange: TNotifyEvent read FOnChange write FOnChange;
    property OnChanging: TNotifyEvent read FOnChanging write FOnChanging;
  end;

implementation

{ TIPList }

procedure TIPList.Changed;
begin
ifFUpdating and Assigned(FOnChange) then
FOnChange(Self);
end;

procedure TIPList.Changing;
begin
ifFUpdating and Assigned(FOnChanging) then
FOnChanging(Self);
end;

function TIPList.IPIntToIPStr(Value: TIPInt): TIPStr;
begin
Result.A1 := IntToStr(Value and $ff000000 shr 24);
Result.A2 := IntToStr(Value and $00ff0000 shr 16);
Result.A3 := IntToStr(Value and $0000ff00 shr  8);
Result.A4 := IntToStr(Value and $000000ff);
end;

function TIPList.IPStrToIPInt(Value: TIPStr): TIPInt;
begin
Result :=StrToInt(Value.A1);
Result := Result shl 8;
Result := Result or StrToInt(Value.A2);
Result := Result shl 8;
Result := Result or StrToInt(Value.A3);
Result := Result shl 8;
Result := Result or StrToInt(Value.A4);
end;
function TIPList.IPIntToStr(Value: TIPInt): string;
var
IPStr :TIPStr;
begin
IPStr := IPIntToIPStr(Value);
Result := IPStr.A1+'.'+IPStr.A2+'.'+IPStr.A3+'.'+IPStr.A4;
end;

function TIPList.StrToIPInt(Value: string): TIPInt;
```

```
var
sp :Integer;
begin
 // Можно было бы взять inet_addr() из WinSock, но мы воспользуемся своей
 // функцией
sp := Pos('.', Value);
Result :=StrToInt(Copy(Value, 1, sp-1)) shl 24;
System.Delete(Value, 1, sp);
sp := Pos('.', Value);
Result := Result or (StrToInt(Copy(Value, 1, sp-1)) shl 16);
System.Delete(Value, 1, sp);
sp := Pos('.', Value);
Result := Result or (StrToInt(Copy(Value, 1, sp-1)) shl 8);
System.Delete(Value, 1, sp);
Result := Result or StrToInt(Trim(Value));
end;

procedure TIPList.Grow;
var
  Delta: Integer;
begin
 // Если размер списка больше 4 кБ выделяем сразу по 1024 записей
ifFLength> 1024 then Delta := 1024 else
Delta := 256;
FLength :=FLength + Delta;
SetLength(FIPItemList, FLength);
end;

procedure TIPList.UpdateMem;
begin
 // Еслитребуетсяещепамять - выделим
 if FLength - FCount = 0 then Grow;
// Если много лишней памяти - укоротим
if FLength - FCount> 10*1024 then
SetLength(FIPItemList, FCount+1024);
end;

function TIPList.Get(Index: Integer): string;
begin
if (Index < 0) or (Index >= FCount) then Error(@SListIndexError, Index);
Result :=IPIntToStr(FIPItemList[Index]);
end;

function TIPList.GetIPInt(Index: Integer): TIPInt;
begin
if (Index < 0) or (Index >= FCount) then Error(@SListIndexError, Index);
Result :=FIPItemList[Index];
end;

function TIPList.GetIPStr(Index: Integer): TIPStr;
begin
if (Index < 0) or (Index >= FCount) then Error(@SListIndexError, Index);
Result :=IPIntToIPStr(FIPItemList[Index]);
```

```
end;

function TIPList.GetCount: Integer;
begin
Result :=FCount;
end;

procedure TIPList.Put(Index: Integer; const S: string);
begin
 // Добавляем всегда только в конец списка
UpdateMem;
 Changing;
FIPItemList[FCount] := StrToIPInt(S);
Inc(FCount);
 Changed;
end;

procedure TIPList.PutIPInt(Index: Integer; const S: TIPInt);
begin
UpdateMem;
 Changing;
FIPItemList[FCount] := S;
Inc(FCount);
 Changed;
end;

procedure TIPList.PutIPStr(Index: Integer; const S: TIPStr);
begin
 // Добавляем всегда только в конец списка
UpdateMem;
 Changing;
FIPItemList[FCount] := IPStrToIPInt(S);
Inc(FCount);
 Changed;
end;

procedure TIPList.Insert(Index: Integer; const S: string);
begin
Put(0, S);
end;

procedure TIPList.SetUpdateState(Updating: Boolean);
begin
FUpdating := Updating;
end;

procedure TIPList.Clear;
begin
FCount := 0;
UpdateMem;
end;

procedure TIPList.Delete(Index: Integer);
```

```
begin
 // Поставим на место удаляемого элемента последний и уменьшим FCount
if (Index < 0) or (Index >= FCount) then Error(@SListIndexError, Index);
 Changing;
FIPItemList[Index] := FIPItemList[FCount-1];
Dec(FCount);
 Changed;
end;

function TIPList.Add(const S: string): Integer;
begin
Put(0, S);
Result := FCount-1;
end;

procedure TIPList.Exchange(Index1, Index2: Integer);
var
VarVal :TIPInt;
begin
if (Index1 < 0) or (Index1 >= FCount) then Error(@SListIndexError, Index1);
if (Index2 < 0) or (Index2 >= FCount) then Error(@SListIndexError, Index2);
 Changing;
VarVal :=FIPItemList[Index1];
FIPItemList[Index1] := FIPItemList[Index2];
FIPItemList[Index2] := VarVal;
 Changed;
end;

function TIPList.EnumChaptNums(Mask: string; CallBack: TCNCallBack; Prefix: string):
Integer;
var
a, b : Byte;
s    : string;
i    :Integer;
begin
Mask := Trim(Mask);
Result := 0;
ifPos('*', Mask) > 0 then
begin
fori := Low(Byte) to High(Byte) do
if @CallBack<> nil then CallBack(i, Prefix, Self);
Result := High(Byte) + 1;
    Exit;
  end;

ifPos(',', Mask) > 0 then
whilePos(',', Mask) > 0 do
begin
s := Trim(Copy(Mask, 1, Pos(',', Mask)-1));
Result := Result + EnumChaptNums(s, CallBack, Prefix);
System.Delete(Mask, 1, Pos(',', Mask));
end;
```

```
        ifPos('-', Mask) > 0 then
        try
        a := StrToInt(Trim(Copy(Mask, 1, Pos('-', Mask)-1)));
        s := Trim(Copy(Mask, Pos('-', Mask)+1, 255));
        fori := 1 to Length(s) do
              if not (s[i] in ['0'..'9']) then
                begin
        SetLength(s, i-1);
                  Break;
        end;
        b := StrToInt(Trim(s));
        fori := a to b do
        if @CallBack<> nil then CallBack(i, Prefix, Self);
        Result := Result + b-a + 1;
            Exit;
        except
        Result := -1;
        Exit;
        end;

        try
        a := StrToInt(Mask);
        if @CallBack<> nil then CallBack(a, Prefix, Self);
        Result := Result + 1;
         except
        Result := -1;
           raise EListError.CreateFmt('TIPList: Error on Parsing IP mask', []);
         end;
        end;

        procedure ChaptNumsStub4(Num: Byte; Prefix: string; Obj: Pointer);
        begin
         if Obj = nil then Exit;
        TIPList(Obj).Put(0, Prefix + IntToStr(Num));
        end;

        procedure ChaptNumsStub3(Num: Byte; Prefix: string; Obj: Pointer);
        begin
         if Obj = nil then Exit;
        TIPList(Obj).EnumChaptNums(TIPList(Obj)._A4,        ChaptNumsStub4,        Prefix        +
IntToStr(Num)+'.');
        end;

        procedure ChaptNumsStub2(Num: Byte; Prefix: string; Obj: Pointer);
        begin
         if Obj = nil then Exit;
        TIPList(Obj).EnumChaptNums(TIPList(Obj)._A3,        ChaptNumsStub3,        Prefix        +
IntToStr(Num)+'.');
        end;

        procedure ChaptNumsStub1(Num: Byte; Prefix: string; Obj: Pointer);
        begin
        TIPList(Obj).EnumChaptNums(TIPList(Obj)._A2, ChaptNumsStub2, IntToStr(Num)+'.');
```

```
end;

function TIPList.ProcessSingleMask(Mask: string): Integer;
var
i  : Integer;
AA : array[0..3] of string;
begin
try
Result :=Self.Count;
ifPos('.', Mask) > 0 then
begin
i := 0;
while (Pos('.', Mask) > 0) and (i< 4) do
begin
AA[i] := Trim(Copy(Mask, 1, Pos('.', Mask)-1));
Inc(i);
System.Delete(Mask, 1, Pos('.', Mask));
        end;
       AA[i] := Trim(Mask);
     end;
   _A1 := AA[0];
   _A2 := AA[1];
   _A3 := AA[2];
   _A4 := AA[3];
ifEnumChaptNums(_A1, ChaptNumsStub1, '') = -1 then
     raise EListError.CreateFmt('TIPList: Error on Parsing IP mask', []);
 except
   Beep;
   raise EListError.CreateFmt('TIPList: Error on Parsing IP mask', []);
 end;
Result :=Self.Count - Result;
end;

function TIPList.ParseMask(Mask: string): Integer;
var
i, dP : Integer;
sMask : string;
begin
Result :=Self.Count;
dP := Pos(';', Mask);
 while dP> 0 do
   begin
sMask := Copy(Mask, 1, dP-1);
System.Delete(Mask, 1, dP);

ProcessSingleMask(sMask);

dP := Pos(';', Mask);
   end;
ProcessSingleMask(Mask);
Result :=Self.Count - Result;
end;
end.
```