Инженерный вестник Дона, №2 (2022)
ivdon.ru/ru/magazine/archive/n2y2022/7475

Моделирование процессов функционирования системы электронного документооборота при воздействии ARP-spoofing атак

Н.В. Шишов[1], *В.А. Ломазов*[2,3]

[1]*Белгородский университет кооперации, экономики и права,*
[2]*Белгородский государственный аграрный университет им. В.Я. Горина,*
[3]*Белгородский государственный национальный исследовательский университет*

Аннотация: В статье рассматривается проблема исследования функционирования системы электронного документооборота при несанкционированных воздействиях, актуальность и практическая значимость которой обусловлена как особенностью требований по обеспечению защиты конфиденциальной информации, так и значимостью ущерба при нарушении бесперебойного протекания документов, циркулирующих в системе. Для моделирования процессов функционирования системы электронного документооборота предложен подход, основанный на использовании аппарата сетей Петри-Маркова, позволяющий учесть статистический характер процессов поступления документов на обработку и проявления воздействий от преднамеренных угроз безопасности информации. В рамках предложенного подхода разработана модель функционирования системы электронного документооборота при воздействии ARP-spoofing атак, являющихся распространенным видом угроз для информационных систем сферы государственного управления. При этом рассмотрены варианты воздействия угроз при отсутствии технических средств защиты информации и их применении. Построенная модель может быть использована при проведении вычислительных экспериментов по определению наиболее эффективных средств защиты информации систем электронного документооборота.
Ключевые слова: система электронного документооборота, несанкционированное воздействие, имитационное моделирование, сети Петри-Маркова.

Введение. В условиях постоянного совершенствования информационных технологий и их внедрения в повседневную жизнь общества особую значимость принимает защита конфиденциальной информации.

Согласно [1], система электронного документооборота (далее – СЭД) – это организационно-техническая система, предоставляющая возможность централизованной обработки циркулирующих в организации документов. Ресурсы СЭД обязаны отвечать текущему положению организаций и нуждаются в периодической модернизации.

В соответствии с методическим документом ФСТЭК России «Методика оценки угроз безопасности информации» от 5 февраля 2021 года,

конфиденциальная информация, находящая в СЭД, способна вызвать интерес у многого количества лиц, начиная с авторизованных пользователей систем и сетей, сотрудников конкурентных организаций, отдельных физических лиц (хакеров), а также представителей зарубежных спецслужб.

При этом в утвержденных государственными регуляторами в области защиты информации нормативно-правовых актах (далее – НПА), в частности, приказе ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года № 17, не определены требования к системам электронного документооборота в отношении защиты от угроз информационной безопасности. Имеющиеся НПА определяют требования к информационным системам в целом, при этом, не учитывая особенностей СЭД.

Поскольку на процессы обработки документов в СЭД значительное воздействие оказывает большое количество различных факторов (свойства конкретного документа, характеристика системного программного обеспечения, а также характер реализации атак), то для оценки эффективности систем защиты информации необходимо провести моделирование протекающих процессов в СЭД [2,3].

Рассмотрению проблематики моделирования систем информационной безопасности посвящено достаточно большое количество работ (например, [4-6]). Однако, как было выявлено в ходе анализа опубликованных материалов, применяемые подходы ориентированы на реализацию ограниченного функционала средств защиты информации при одновременном осуществлении атак нарушителями и не предусматривают динамических изменений в СЭД под воздействием угроз.

Таким образом, исследуемая в настоящей работе проблема моделирования процессов функционирования системы документооборота

при воздействии ARP-spoofing атак является актуальной и практически значимой.

Материалы и методы. Для описания сложных процессов функционирования СЭД целесообразно применять графические модели, обладающие высокой наглядностью [7]. При моделировании функционирования систем с большим количеством вероятных состояний и переходов (к которым может быть отнесена СЭД) важным требованием является учет таких факторов, как статистическая неопределенность времени выполнения и параллелизм протекающих внутри СЭД процессов, а также непредсказуемый порядок осуществления переходов между возможными состояниями. С учетом этого для моделирования процесса функционирования СЭД под воздействием угроз предлагается использовать аппарат сетей Петри-Маркова.

Сеть Петри-Маркова может быть формально представлена в виде [8]:

$$\theta = <П,M>,$$

где $П$ – сеть Петри, определяющая структуру сети Петри-Маркова, а M – случайный процесс, накладываемый на структуру $П$.

Структура сети Петри-Маркова может быть представлена в виде:

$$П = <A,Z,I_z(A),O_z(A)>,$$

где A – конечное множество позиций; Z – конечное множество переходов; $I_A(Z)$ – входная функция переходов, и $O_A(Z)$ – входная функция позиций.

Граф сети Петри-Маркова представлен на рис. 1.

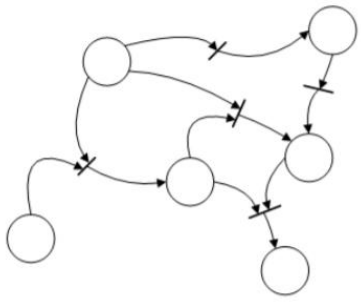

Рис. 1. – Сеть Петри-Маркова

Сеть Петри (отражающая структуру сети Петри-Маркова) представляет собой двудольный направленный граф, состоящий из вершин (позиции и переходы), при этом имеет входные и выходные функции.

Графически позиции отмечаются кружками, а переходы – чертой. Возможность выполнения того или иного шага отмечается направленной дугой (стрелкой). Множества, не обладающие входящими дугами, называются входными, а множества, не имеющие исходящих – выходными.

Приведение в действие переходов обусловлено числом входящих дуг, а также числом дуг, соответствующих определенным условиям «И», «ИЛИ», «НЕ» (рис. 2).

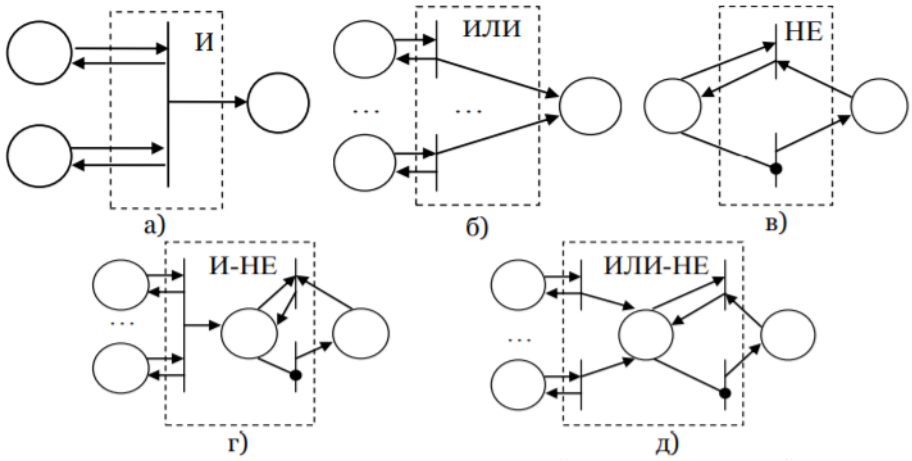

Рис. 2. – Переходы, используемые при моделировании процессов: а) элемент «И»; б) элемент «ИЛИ»; в) элемент «НЕ»; г) элемент «И-НЕ»; д) элемент «ИЛИ-НЕ»

Результаты. Для моделирования реализации угроз безопасности используются различные состояния системы защиты информации, а переходы представляют возможные процессы злоумышленников, действующих в одной и той же системе (и, следовательно, в одной и той же сети Петри-Маркова).

Рассмотрим проведение атаки на примере реализации ARP-spoofing, в ходе которой происходит преобразование IP-адресов и MAC-адресов (рис. 3).

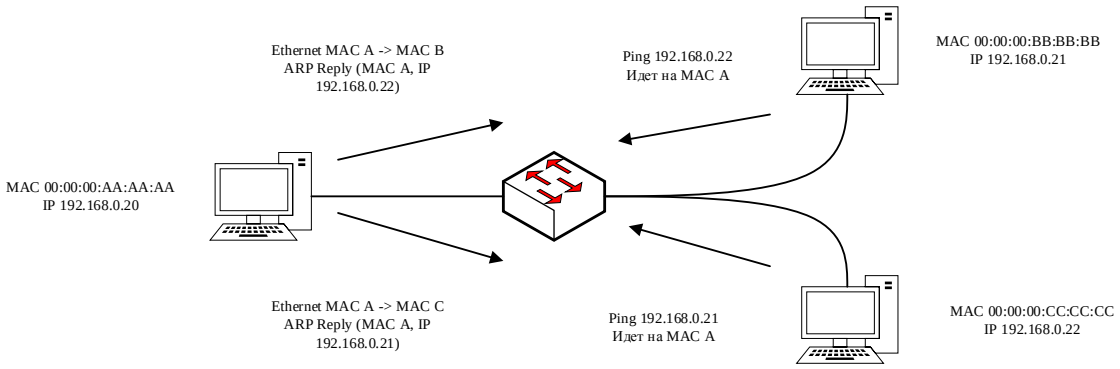

Рис. 3. – Реализация ARP-spoofing атаки

В случае применения в распределенной сети алгоритма удаленного поиска возникает вероятность реализации типовой атаки с использованием протокола ARP. Согласно [9,10], осуществив перехват широковещательного сообщения (ARP-запроса), возможно направить ложный ARP-ответ, оповестив атакуемый узел, о том, что являешься искомым узлом с целью последующего контроля сетевого трафика.

Вид сети Петри-Маркова, описывающей основные этапы процессов СЭД без применения средств защиты информации, представлен на рис. 4.

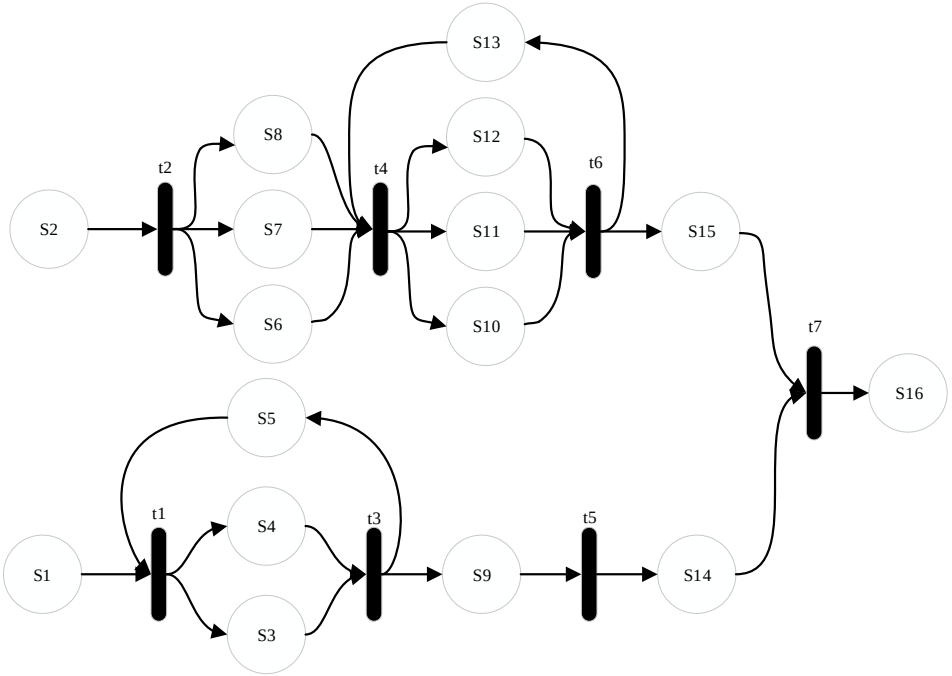

Рис. 4. – Вид сети Петри-Маркова, моделирующей атаку «ARP-spoofing» без применения средств защиты информации

Описание позиций и переходов сети Петри-Маркова, моделирующей функционирование СЭД под воздействием ARP-spoofing атаки (при использовании и без использования средств защиты информации) приведено в таблице № 1.

Таблица № 1

Описание позиций и переходов сети Петри-Маркова, моделирующей функционирование СЭД под воздействием ARP-spoofing атаки

Обозначение	Описание
s_1	Исполнитель подготовил отчет об исполнении
s_2	Узел злоумышленника готов к проведению атаки
s_3	Руководитель структурного подразделения получил отчет об исполнении
s_4	Руководитель организации получил отчет об исполнении
s_5	Исполнитель дорабатывает отчет об исполнении
s_6	Запрос получен маршрутизатором
s_7	Запрос получен узлом «1» клиента СЭД
s_8	Запрос получен узлом «2» клиента СЭД
s_9	Отчет об исполнении согласован
s_{10}	Смена MAC-адреса на узле «1» клиента СЭД завершена
s_{11}	Смена MAC-адреса на узле «2» клиента СЭД завершена
s_{12}	Смена MAC-адресов на маршрутизаторе завершена
s_{13}	Злоумышленник готов к повторной подмене MAC-адресов
s_{14}	Исходящий документ зарегистрирован и направлен адресату посредством маршрутизатора
s_{15}	ARP-таблица атакуемого узла изменена
s_{16}	Финальное состояние: атака успешно реализована
t_1	Отчет об исполнении направлен на согласование с руководителями
t_2	Формируется широковещательное сообщение всем узлам СЭД
t_3	Логический переход, срабатывающий при условии, что отчет об исполнении согласован всеми руководителями
t_4	Злоумышленник проводит смену MAC-адресов
t_5	Регистрация исходящего документа и отправка адресату
t_6	Переход срабатывает при условии, что подмена MAC-адресов в позициях S11, S12, S13 проведена успешно
t_7	ARP-таблица атакуемого узла изменена и исходящий документ поступил на маршрутизатор

Вид сети Петри-Маркова, описывающей основные этапы процессов СЭД с применением средств защиты информации, представлен на рис. 5.

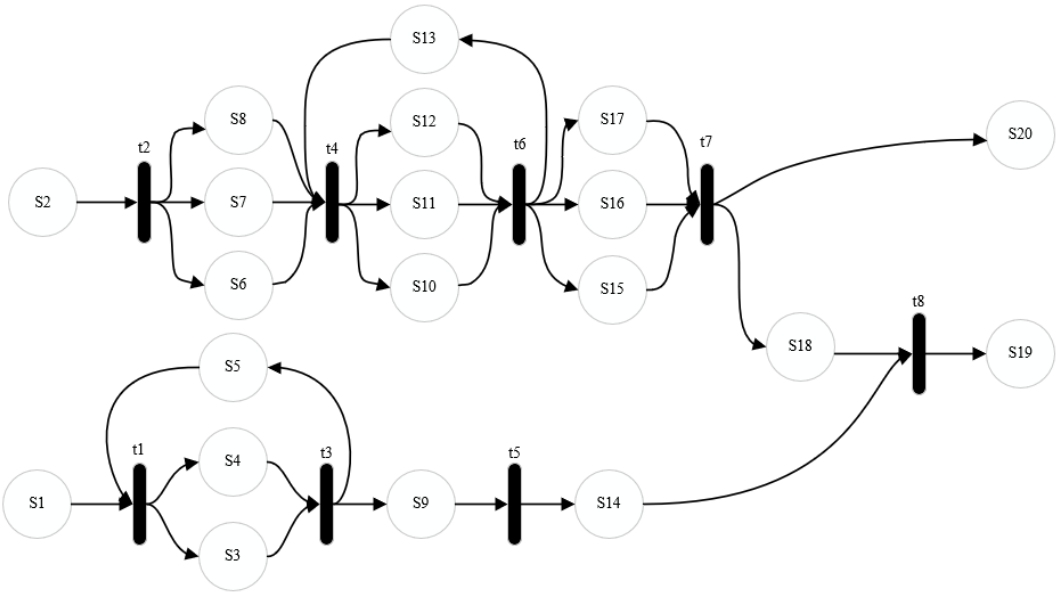

Рис. 5. – Вид сети Петри-Маркова, моделирующей атаку «ARP-spoofing» при применении средств защиты информации

Для предотвращения несанкционированных воздействий, вызванных атакой типа «ARP-spoofing», необходимо проводить сканирование сети с построением списка устройств и их свойств. Для проведения таких мероприятий можно использовать arpwatch – для операционных систем на базе ядра Linux, ARP Monitor – Windows. В соответствии с [11], принцип работы такого рода программ заключается в формировании журнала событий, который отслеживает пары IP-адресов с MAC-адресами с отметкой во времени и сообщает о возникших изменениях.

При использовании средств защиты информации модель претерпевает следующие изменения: на позициях S_{15}-S_{17} – происходит проверка смены MAC-адреса на «1», «2» узле и маршрутизаторе; t_7 – логический переход срабатывает в зависимости от результата проверки подмены; S_{18} – ARP-таблица атакуемого узла изменена; S_{19}, S_{20} – Финальное состояние: атака успешно реализована и финальное состояние: средство защиты отразило

атаку, соответственно; t_8 – ARP-таблица атакуемого узла изменена и исходящий документ поступил на маршрутизатор.

Заключение. Внедрение системы защиты СЭД, представляющее собой совокупность взаимосвязанных правовых, организационных и технических процессов, связано со значительными затратами, в то время как (в ряде случаев) эффективность защиты не является очевидной.

В связи с этим, для поддержки принятия научно обоснованных управленческих решений по обеспечению информационной безопасности СЭД, целесообразно проведение имитационных вычислительных экспериментов на базе моделей функционирования СЭД под действием атак.

Построенная в настоящей работе модель функционирования СЭД базируется на использовании аппарата сетей Петри-Маркова, что обеспечивает высокий уровень наглядности при анализе вычислительных экспериментов, направленных на определение наиболее эффективных средств защиты информации систем электронного документооборота.

Литература

1. Azad A. Implementing electronic document and record management systems. 1st Edition. New York: Auerbach Publications, 2008. 280 p.

2. Андреев Д.А., Панфилов А.Н., Скоба А.Н. Управление операционными процессами операторов сложных систем // Инженерный вестник Дона. 2017. №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4322.

3. Перепелкина О.А. Математическое моделирование системы электронного документооборота и делопроизводства в исполнительных органах государственной власти на примере Пензенской области // Науковедение. 2017. №6, URL: elibrary.ru/item.asp? id=32598229.

4. Гостищева Т.В., Ломазов В.А., Малий Ю.В. Модели и методы проектирования систем защиты информации. Белгород: Издательство Белгородского университета кооперации, экономики и права, 2021. 175 с.

5. Ломазов В.А., Ломазова В.И., Ломакин В.В., Асадуллаев Р.Г. Процедура оценки защищенности интегрированной платформы разработки корпоративных приложений // Современная наука и инновации. 2019. №3. С. 145-148.

6. Ломазов В.А., Гостищева Т.В., Пономарев Д.В. Эволюционный синтез иерархии оценочных показателей проекта в сфере информационной безопасности // Глобальный научный потенциал. 2017. №11. С. 86-88.

7. Kajdanowicz T., Kazienko P., Indyk W. Parallel processing of large graphs // Future Generation Computer Systems. 2014. V. 32. pp. 324-337.

8. Ivutin A.N., Larkin E.V., Lutskov Y.I., Novikov A.S. Simulation of concurrent process with Petri-Markov nets // Life Science Journal. 2014. №11, URL: lifesciencesite.com/lsj/life1111/086_25899life111114_506_511.pdf.

9. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона. 2019. №4. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

10. Hong S., Oh M., Lee S. Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA // Mathematical and Computer Modelling. 2013. №58. p. 254-260.

11. Ramachandran V., Nandi S. Detecting ARP Spoofing: An Active Technique // International Conference on Information Systems Security. 2005. V. 3803. pp. 239-250.

References

1. Azad A. Implementing electronic document and record management systems. 1st Edition. New York: Auerbach Publications, 2008. 280 p.

2. Andreev D.A., Panfilov A.N., Skoba A.N. Inzhenernyj vestnik Dona. 2017, №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4322.

3. Perepelkina O.A. Naukovedenie. 2017, №6. URL: elibrary.ru/item.asp?id=32598229.

4. Gostishcheva T.V., Lomazov V.A., Malij YU.V. Modeli i metody proektirovaniya sistem zashchity informacii. [Models and methods for designing information security systems]. Belgorod: Izdatel'stvo Belgorodskogo universiteta kooperacii, ekonomiki i prava, 2021. 175 p.

5. Lomazov V.A., Lomazova V.I., Lomakin V.V., Asadullaev R.G. Sovremennaya nauka i innovacii. 2019, №3. pp. 145-148.

6. Lomazov V.A., Gostishcheva T.V., Ponomarev D.V. Global'nyj nauchnyj potencial. 2017, №11. pp. 86-88.

7. Kajdanowicz T., Kazienko P., Indyk W. Future Generation Computer Systems. 2014. V. 32. pp. 324-337.

8. Ivutin A.N., Larkin E.V., Lutskov Y.I., Novikov A.S. Life Science Journal. 2014. №11, URL: lifesciencesite.com/lsj/life1111/086_25899life111114_506_511.pdf.

9. Menciev A.U., CHebieva H.S. Inzhenernyj vestnik Dona. 2019, №4.URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

10. Hong S., Oh M., Lee S. Mathematical and Computer Modelling. 2013. №58. p. 254-260.

11. Ramachandran V., Nandi S. International Conference on Information Systems Security. 2005. V. 3803. pp. 239-250.