МОДЕЛИРОВАНИЕ APT-АТАК, ЭКСПЛУАТИРУЮЩИХ УЯЗВИМОСТЬ ZEROLOGON

Будников С.А.[1], Бутрик Е.Е.[2], Соловьев С.В.[3]

Цель работы: *разработка модели процесса проведения многоэтапной целенаправленной компьютерной атаки, эксплуатирующей уязвимость Zerologon, основанной на представлении атаки марковским случайным процессом с дискретными состояниями и непрерывным временем.*

Методы исследования: *для формализации атаки в модели используются методы теории марковских процессов, теории вероятностей, вычислительной математики, а также теории графов.*

Новизна: *применение методов вычислительной математики для функционального анализа результатов решения системы уравнений Колмогорова позволяет известными методами анализа непрерывных функций решать задачу максимизации времени устойчивого функционирования критической информационной инфраструктуры при проведении в отношении нее компьютерных атак.*

Результат: *сформулирована общая постановка задачи моделирования процесса проведения многоэтапной целенаправленной компьютерной атаки с использованием системы уравнений Колмогорова, описывающей вероятности нахождения в состояниях конфликта системы безопасности с нарушителем. Методом Адамса, реализованным в среде Mathcad, получены численные решения в зависимости от времени. Введен показатель эффективности системы безопасности значимого объекта критической информационной инфраструктуры как отношение вероятности срабатывания системы безопасности и блокирования действий нарушителя в ходе атаки к вероятности успешного завершения атаки нарушителем. Приводится пример исследования реализации компьютерной атаки в типовой информационной инфраструктуре, включающей корпоративную сеть с доменной архитектурой и автоматизированную систему управления технологическим процессом. Для рассмотренного примера определены оптимальные значения временных параметров системы безопасности. При реализации мер защиты с обоснованными вероятностно-временными характеристиками доказано увеличение времени устойчивого функционирования критической информационной инфраструктуры с 11 до 189 ч.*

Практическая значимость: *результаты исследования можно использовать при проектировании и тестировании систем безопасности значимых объектов критической информационной инфраструктуры с учетом задаваемых параметров системы безопасности и нарушителя.*

Ключевые слова: *значимый объект, компьютерная атака, критическая информационная инфраструктура, марковский процесс, система безопасности.*

DOI:10.21681/2311-3456-2021-6-47-61

Введение

В настоящее время вопросы безопасности информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления субъектов критической информационной инфраструктуры (КИИ) приобретают важное значение. Форсирование создания систем безопасности значимых объектов КИИ определяется не только требованиями нормативно-правовых и руководящих документов в области информационной безопасности[4], но и резким ростом количества сообщений о компьютерных инцидентах на объектах КИИ Российской Федерации[5], а также на объектах информационной инфраструктуры зарубежных стран[6].

В этих условиях особенно важными являются вопросы оценки эффективности создаваемых систем безопасности значимых объектов КИИ. Поэтому в ходе проектирования системы безопасности значимого объекта в целях тестирования рекомендовано ее макетирование или создание тестовой среды с использованием средств и методов моделирования.

Необходимость оценки эффективности создаваемых систем безопасности значимых объектов КИИ

4 Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. 2021. – URL: https://docs.cntd.ru/document/542616931 (дата обращения: 15.09.2021).

5 APT-атаки на промышленные компании в России. Обзор тактик и техник, Positive Technologies, 2019. // Positive Technologies [Электронный ресурс]. 2019. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-industry-2019/ (дата обращения: 15.09.2021)

6 2020 Cybersecurity threat trends outlook // [Электронный ресурс]. 2020. – URL: https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/ (дата обращения: 01.07.2021).

1 Будников Сергей Алексеевич, доктор технических наук, доцент, главный научный сотрудник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», Воронеж, Россия. E–mail: buser@bk.ru

2 Бутрик Екатерина Евгеньевна, аспирант ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Воронеж, Россия. E-mail: keit1991@list.ru.

3 Соловьев Сергей Вениаминович, кандидат технических наук, доцент, начальник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», Воронеж, Россия. E–mail: sersol@mail.ru.

определяет потребность в разработке простых и адекватных математических моделей реализации компьютерных атак. Использование методов математического моделирования в ходе проектирования системы безопасности значимого объекта позволяет без значительных затрат и влияния на функционирование объекта обосновать требования к системе в целом или ее отдельным частям.

Проведённый анализ методического обеспечения [1-10], применяемого при исследовании в области обеспечения компьютерной безопасности, показал, что в случае сложных систем, к которым относятся значимые объекты КИИ, наиболее подходящими методами и подходами к моделированию компьютерных атак являются использование теории сетей Петри-Маркова [11] и марковских случайных процессов [12].

Одним из наиболее опасных сценариев целенаправленных программных воздействий на объекты КИИ и сети электросвязи в настоящее время считается компьютерная атака, реализуемая путем эксплуатации уязвимости BDU:2020-04016 Zerologon (CVE-2020-1472) [13]. Эта уязвимость основана на дефекте в реализации процедур аутентификации на контроллере домена и позволяет нарушителю получить привилегий администратора домена Active Directory и затем реализовать внедрение полезной нагрузки (скрипта). Указанный дефект присутствует в реализации криптографического преобразования, используемого при аутентификации в протоколе Microsoft Windows Netlogon Remote Protocol (MS-NRPC)[7], используемый для связи рабочих станций и серверов с контроллерами домена по защищенному каналу. Атака Zerologon реализуется путем сброса пароля учетной записи Active Directory контроллера домена в сетевом домене в пустую строку. Это позволяет не прошедшему проверку подлинности нарушителю с сетевым доступом к контроллеру домена аутентифицироваться и получить доступ к командной консоли на другом или этом же контроллере домена и полностью контролировать весь объект КИИ. Поэтому в качестве тестового программного воздействия на объекты КИИ при моделировании будем рассматривать именно компьютерную атаку, эксплуатирующую уязвимость Zerologon.

Постановка задачи

Целью работы является разработка модели процесса проведения многоэтапной целенаправленной компьютерной атаки, так называемой атаки типа Advanced persistent threat (APT-атаки), эксплуатирующей уязвимость Zerologon, основанной на представлении ее случайным марковским процессом с дискретными состояниями и непрерывным временем.

В ходе реализации подобной атаки с различными вариантами деструкции (векторами атак) нарушитель должен успешно пройти следующие этапы:

- получение доступа (физического или удаленного) к сети КИИ;
- сканирование ресурсов корпоративной локальной вычислительной сети (ЛВС) с целью получения сведений об IP-адресах контроллеров домена, их *NetBIOS*-именах, названиях домена (доменов);
- извлечение из дампа памяти машинного аккаунта контроллера домена и повышение прав доступа в атакуемом домене;
- эскалация привилегий администратора домена и внедрение полезной нагрузки (скрипта);
- удаленное подключение к автоматизированному рабочему месту (АРМ) оператора технологической установки;
- поиск файлов, содержащих проекты управления, на АРМ оператора технологической установки;
- блокирование доменной учетной записи оператора технологической установки;
- удаленное выключение АРМ оператора объекта КИИ.

Модель процесса проведения многоэтапной целенаправленной компьютерной атаки, эксплуатирующей уязвимость Zerologon

Поскольку разветвлений и соответствующих им логических условий реализации компьютерной атаки, эксплуатирующей уязвимость Zerologon, нет, то для ее моделирования может быть использован аппарат марковских случайных процессов.

С учетом подходов к моделированию операций по схеме марковских случайных процессов [14], в ходе этой атаки моделируемая система может находиться во множестве дискретных состояний $S_0, S_1, \ldots, S_n$, переход (перескок) системы S из состояния в состояние может осуществляться в любой момент времени.

Как отмечалось выше, в ходе реализации данной атаки нарушитель должен успешно пройти этапы, детализированные в таблице 1. Название используемых злоумышленником тактик взяты из базы данных атак и средств защиты - MITRE Att&ck (Adversarial Tactics, Techniques, and Common Knowledge - тактики, техники и общие знания)[8].

Тогда, с учетом сделанных заключений и ассоциативной формализации номера состояния (см. таблицу 1), можно разметить граф состояний системы безопасности, вершины которого отражают состояния в ходе атаки в любой момент времени t, а дуги графа — направление протекания процесса. Анализ данного графа показал, что, осуществляя свертку графа путем объединения последовательных групп вершин, можно снизить его размерность и сократить количество вершин с 20 до 14. Свёрнутый граф атаки, эксплуатирующей уязвимость Zerologon, представлен на рис. 1.

Поясним принятые обозначения. Вершина S_0, представленного на рис. 1 графа, определяет начальное состояние процесса проведения атаки. Переходные вероятности P_{ij} характеризуют переходы из i-о состояния к j-у состоянию со средним значением времени $\overline{t}_{ij}$.

7 Zerologon: уязвимость в протоколе Netlogon позволяет захватить контроллер домена // 2020. [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/cve-2020-1472-domain-controller-vulnerability/29085 / (дата обращения: 21.11.2020 г.).

8 Официальный сайт MITRE Att&ck // 2021. [Электронный ресурс]. – URL: https://attack.mitre.org/ (дата обращения 25.04.2021 г.).

Таблица 1

Этапы атаки, эксплуатирующей уязвимость Zerologon

№	Обозначение узла	Этапы атаки (состояние графа)
1	S_0	Начало атаки
2	S_1	Проверка готовности и обновления инструментария нарушителя (Kali Linux)
3	S_2	Использование техники «System network configuration discovery» («Сбор информации о конфигурации и настройках сети»). Подключение к сети как DHCP-клиент и определение сетевых параметров
4	S_3	Использование программного средства Wireshark. Перехват пакетов и выявление IP-адресов основных узлов сети путем использования техники «Network Sniffing» («Получение аутентификационных данных путем перехвата и анализа сетевого трафика»)
5	S_4	Поиск контроллера домена путем сканирования SMB-устройств в сети путем использования техники «Network Service Scanning» («Получение информации о списке запущенных служб и о наличии в них уязвимостей, путем сканирования портов»)
6	S_5	Эксплуатация уязвимости Zerologon (BDU:2020-04016) путем использования техники «Exploitation of Remote Services» («Эксплуатация уязвимостей программного обеспечения с целью получения доступа к удаленной системе с помощью сервисов удаленного доступа»)
7	S_6	Замена пароля контроллера домена путем использования техники «Credential Dumping» («Получение аутентификационных данных путем извлечения файлов операционной системы»)
8	S_7	Получение значений HASH от учетной записи «Администратор» с использованием модуля Secretsdump путем использования техники «Pass the Hash» («Получение доступа к информационной системе путем захвата хэша и его повторного использования с целью перехвата сеанса (без раскрытия пароля)»)
9	S_8	Подключение к контроллеру домена от имени учетной записи «Администратор»
10	S_9	Получение доступа к интерактивной консоли на контроллере домена
11	S_{10}	Создание привилегированной учетной записи нарушителя
12	S_{11}	Добавление учетной записи нарушителя в группу администраторов домена путем использования техники «Account Manipulation» («Изменение учетных записей системы или домена»)
13	S_{12}	Поиск АРМ, представляющих интерес для нарушителя, путем использования техники «Account Discovery» («Получение списка учетных записей системы или домена»)
14	S_{13}	Удаленное подключение к АРМ оператора технологической установки
15	S_{14}	Поиск файлов, содержащих проекты управления, на АРМ оператора технологической установки путем использования техники «Remote System Discovery» («Сбор информации о хостах в сети, доступных для реализации протокола удаленного доступа»)
16	S_{15}	Копирование файлов, содержащих проекты управления, с АРМ оператора технологической установки путем использования техники «Remote File Copy» («Удаленное копирование файлов»)
17	S_{16}	Блокирование доменной учетной записи оператора технологической установки ОР-ASUTP
18	S_{17}	Удаленное выключение АРМ оператора путем использования техники «Endpoint Denial of Service» («DoS-атака в конечной точке»)

№	Обозначение узла	Этапы атаки (состояние графа)
19	S_{18}	Срабатывание системы безопасности и блокирование действий нарушителя в ходе атаки
20	S_{19}	Успешное завершение атаки

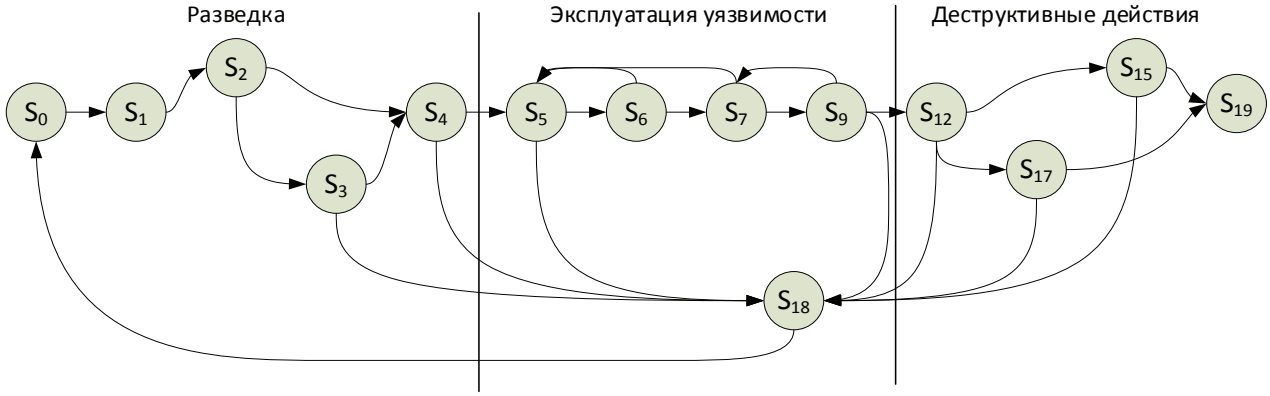

Рис. 1. Свёрнутый граф состояний компьютерной атаки

Таблица 2.

Физический смысл формализуемых переходов

№	Обозначения	Физический смысл события	Временная характеристика	Обозначение	Значение, мин
1	2	3	4	5	6
1	$S_0 \to S_1$	Проверка готовности и обновления инструментария Kali Linux	Среднее время подготовки к атаке	$\overline{t}_{0\_1}$	10
2	$S_1 \to S_2$	Выбор техники «System network configuration discovery». Подключение к сети как DHCP-клиент и определение сетевых параметров	Среднее время определения сетевых параметров	$\overline{t}_{1\_2}$	5
3	$S_2 \to S_3$	Выбор техники «Network Sniffing». Перехват пакетов и выявление IP-адресов основных узлов сети	Среднее время определения сетевых параметров	$\overline{t}_{2\_3}$	8
4	$S_2 \to S_4$	Поиск контроллера домена путем сканирования SMB-устройств в сети, используя технику «Network Service Scanning»	Среднее время поиска контроллеров домена	$\overline{t}_{2\_4}$	10
5	$S_3 \to S_4$	Поиск контроллера домена путем сканирования SMB-устройств в сети, используя технику «Network Service Scanning»	Среднее время поиска контроллеров домена	$\overline{t}_{3\_4}$	10
6	$S_3 \to S_{18}$	Обнаружение средствами защиты информации факта сканирования и его блокирование. Неудача в поиске контроллера домена	Среднее время обнаружения и блокирования процесса сканирования	$\overline{t}_{3\_18}$	8
7	$S_4 \to S_5$	Эксплуатация уязвимости Zerologon (BDU:2020-04016). Техника «Exploitation of Remote Services»	Среднее время эксплуатации уязвимости Zerologon	$\overline{t}_{4\_5}$	12

№	Обозначения	Физический смысл события	Временная характеристика	Обозначение	Значение, мин
8	$S_4 \rightarrow S_{18}$	Обнаружение средствами защиты информации факта эксплуатации уязвимости Zerologon и реализация защитных мер	Среднее время обнаружения факта эксплуатации уязвимости Zerologon	$\overline{t}_{4\_18}$	10
9	$S_5 \rightarrow S_6$	Замена пароля контроллера домена с использованием техники «Credential Dumping»	Среднее время замены пароля контроллера домена	$\overline{t}_{5\_6}$	3
10	$S_5 \rightarrow S_{18}$	Обнаружение средствами защиты информации факта замены пароля контроллера домена, блокирование	Среднее время блокирования замены пароля контроллера домена	$\overline{t}_{5\_18}$	3
11	$S_6 \rightarrow S_5$	Обнаружение средствами защиты информации факта замены пароля контроллера домена, разрыв соединения	Среднее время разрыва соединения с контроллером домена	$\overline{t}_{6\_5}$	9
12	$S_6 \rightarrow S_7$	Получение значений HASH от учетной записи «Администратор» с использованием модуля Secretsdump путем применения техники «Pass the Hash»	Среднее время получения значений HASH	$\overline{t}_{6\_7}$	4
13	$S_7 \rightarrow S_5$	Блокирование получения значений HASH	Среднее время блокирования	$\overline{t}_{7\_5}$	15
14	$S_7 \rightarrow S_9$	Подключение к контроллеру домена от имени учетной записи «Администратор». Получение доступа к интерактивной консоли на контроллере домена	Среднее время доступа к интерактивной консоли на контроллере домена	$\overline{t}_{7\_9}$	5
15	$S_9 \rightarrow S_7$	Блокирование доступа к интерактивной консоли на контроллере домена	Среднее время блокирования доступа к интерактивной консоли	$\overline{t}_{9\_7}$	10
16	$S_9 \rightarrow S_{12}$	Поиск АРМ, представляющих интерес для нарушителя	Среднее время поиска АРМ	$\overline{t}_{9\_12}$	13
17	$S_9 \rightarrow S_{18}$	Блокирование созданной учетной записи нарушителя	Среднее время блокирования созданной учетной записи	$\overline{t}_{9\_18}$	10
18	$S_{12} \rightarrow S_{15}$	Поиск файлов, содержащих проекты управления, на АРМ оператора технологической установки	Среднее время поиска проектов управления	$\overline{t}_{12\_15}$	18
19	$S_{12} \rightarrow S_{17}$	Удаленное выключение АРМ оператора путем использования техники «Endpoint Denial of Service»	Среднее время реализации приемов удаленного выключения АРМ	$\overline{t}_{12\_17}$	5
20	$S_{12} \rightarrow S_{18}$	Блокирование поисковых процедур нарушителя	Среднее время блокирования поисковых процедур злоумышленника	$\overline{t}_{12\_18}$	30
21	$S_{15} \rightarrow S_{19}$	Копирование файлов, содержащих проекты управления	Среднее время копирования файлов, содержащих проекты управления	$\overline{t}_{15\_19}$	30
22	$S_{15} \rightarrow S_{18}$	Блокирование процессов несанкционированного копирования файлов, содержащих проекты управления	Среднее время блокирования процессов несанкционированного копирования файлов, содержащих проекты управления	$\overline{t}_{15\_18}$	20

№	Обозначения	Физический смысл события	Временная характеристика	Обозначение	Значение, мин
23	$S_{17} \to S_{18}$	Блокирование процессов удаленного выключения	Среднее время блокирования процессов удаленного выключения	$\overline{t}_{17\_18}$	10
24	$S_{17} \to S_{19}$	Завершение атаки после выключения АРМ оператора	Среднее время выключения АРМ оператора	$\overline{t}_{17\_19}$	5
25	$S_{18} \to S_0$	Блокирование действий нарушителя, попытка проведения новой атаки	Среднее время начала новой атаки	$\overline{t}_{18\_0}$	100

Понимая, что в случае формализации потоков событий, возникающих в ходе компьютерной атаки, простейшими потоками можно записать систему уравнений Колмогорова, то для получения значений временных характеристик перейдем от значений интенсивностей переходов λ_{ij} к средним значениям времени соответствующего этапа атаки $\overline{t}_{ij}$

$$\lambda_{ij} = \frac{1}{\overline{t}_{ij}}. \quad (1)$$

Исследуемые переходы, физический смысл протекаемых при этом процессов, а также обозначения средних значений времени переходов и их типовые значения приведены в таблице 2.

Для простоты восприятия средних значений времени переходов, переводящих моделируемую систему из одного состояния в другое, связанных с деятельностью сторон, эти значения запишем в виде множества значений времен $\mathbf{T}$. Для графа, представленного на рис. 1, мощность данного множества равна 25, $\{\mathbf{T}\} = 25$, и содержание значений этого множества приведено в графе 6 в таблицы 2.

Как известно из теории марковских процессов с дискретными состояниями и непрерывным временем [12], определение вероятностей событий, характеризующих этапы атаки, требует формализации единого пространства состояний в виде системы уравнений Колмогорова, учитывающей все 25 временных параметров моделируемого процесса. Решение данной системы уравнений позволяет получить зависимости вероятностей нахождения в любом состоянии процесса атаки.

Тогда в нашем случае процесс атаки будет описываться следующей системой однородных дифференциальных уравнений (2)

$$\begin{cases}
\frac{d}{dt}P_{S0}(t) = \frac{s0(t)}{t_{18_0}} - \frac{s0(t)}{t_{0_1}};\\
\frac{d}{dt}P_{S1}(t) = \frac{s0(t)}{t_{0_1}} - \frac{s1(t)}{t_{1_2}};\\
\frac{d}{dt}P_{S2}(t) = \frac{s1(t)}{t_{1_2}} - \left(\frac{s2(t)}{t_{2_3}} + \frac{s2(t)}{t_{2_4}}\right);\\
\frac{d}{dt}P_{S3}(t) = \frac{s2(t)}{t_{2_3}} - \left(\frac{s3(t)}{t_{3_4}} + \frac{s3(t)}{t_{3_18}}\right);\\
\frac{d}{dt}P_{S4}(t) = \frac{s2(t)}{t_{2_4}} + \frac{s3(t)}{t_{3_4}} - \left(\frac{s4(t)}{t_{4_5}} + \frac{s4(t)}{t_{4_18}}\right);\\
\frac{d}{dt}P_{S5}(t) = \frac{s4(t)}{t_{4_5}} + \frac{s6(t)}{t_{6_5}} + \frac{s7(t)}{t_{7_5}} - \left(\frac{s5(t)}{t_{5_6}} + \frac{s5(t)}{t_{5_18}}\right);\\
\frac{d}{dt}P_{S6}(t) = \frac{s5(t)}{t_{5_6}} - \left(\frac{s6(t)}{t_{6_5}} + \frac{s6(t)}{t_{6_7}}\right);\\
\frac{d}{dt}P_{S7}(t) = \frac{s6(t)}{t_{6_7}} + \frac{s9(t)}{t_{9_7}} - \left(\frac{s7(t)}{t_{7_5}} + \frac{s7(t)}{t_{7_9}}\right);\\
\frac{d}{dt}P_{S9}(t) = \frac{s7(t)}{t_{7_9}} - \left(\frac{s9(t)}{t_{9_7}} + \frac{s9(t)}{t_{9_12}} + \frac{s9(t)}{t_{9_18}}\right);\\
\frac{d}{dt}P_{S12}(t) = \frac{s9(t)}{t_{9_12}} - \left(\frac{s12(t)}{t_{12_15}} + \frac{s12(t)}{t_{12_17}} + \frac{s12(t)}{t_{12_18}}\right);\\
\frac{d}{dt}P_{S15}(t) = \frac{s12(t)}{t_{12_15}} - \left(\frac{s15(t)}{t_{15_18}} + \frac{s15(t)}{t_{12_19}}\right);\\
\frac{d}{dt}P_{S17}(t) = \frac{s12(t)}{t_{12_17}} - \left(\frac{s17(t)}{t_{17_18}} + \frac{s17(t)}{t_{17_19}}\right);\\
\frac{d}{dt}P_{S18}(t) = \frac{s3(t)}{t_{3_18}} + \frac{s4(t)}{t_{4_18}} + \frac{s5(t)}{t_{5_18}} + \frac{s9(t)}{t_{9_18}} + \\
\qquad + \frac{s12(t)}{t_{12_18}} + \frac{s15(t)}{t_{15_18}} + \frac{s17(t)}{t_{17_18}} - \frac{s18(t)}{t_{18_0}};\\
\frac{d}{dt}P_{S19}(t) = \frac{s15(t)}{t_{15_19}} + \frac{s17(t)}{t_{17_19}};
\end{cases} \quad (2)$$

для заданных начальных условий

$$P_{S0}(0)=1, P_{S1}(0)=0, P_{S2}(0)=0, P_{S3}(0)=0,$$
$$P_{S4}(0)=0, P_{S5}(0)=0, P_{S6}(0)=0, P_{S7}(0)=0,$$
$$P_{S9}(0)=0, P_{S12}(0)=0, P_{S15}(0)=0, P_{S17}(0)=0,$$
$$P_{S18}(0)=0, P_{S19}(0)=0.$$

Аналитическое решение данной системы возможно с использованием различных методов решения однородных дифференциальных уравнений первого порядка (метод исключения, Эйлера, операторным методом), но результаты решения относительно всех исследуемых переменных представляют сложные выражения, а процесс нахождения решения будет достаточно трудоемким. Развитие численных методов и их современная реализация в доступных средах моделирования позволяют получить достаточно быстро решение искомой задачи в виде функции, с которой допустимы операции дифференцирования и интегрирования [15]. Это составляет основу для решения поставленной в работе задачи.

Для решения данной системы однородных дифференциальных уравнений используем конечноразностный многошаговый метод численного интегрирования обыкновенных дифференциальных уравнений первого

Таблица 3

Временные характеристики мер защиты информации

№	Обозначение	Характеристика	Формализуемый переход на рис. 1	Обозначение в Таблице 2	Типовое значение параметра, мин
1	t_{DHCP}	Среднее время срабатывания меры защиты от подключения стороннего *DHCP*-клиента	$S_1 \to S_2$	$\overline{t}_{0\_1}$	5
2	$t_{\text{WireShark}}$	Среднее время срабатывания меры защиты от сниффинга	$S_2 \to S_3$	$\overline{t}_{2\_3}$	8
3	t_{SMB}	Среднее время срабатывания меры защиты от сканирования *SMB* ресурсов	$S_2 \to S_4$	$\overline{t}_{2\_4}$	10
4	$t_{\text{Zerologon}}$	Среднее время применения патча и рекомендаций *Microsoft* по удалению уязвимости	$S_4 \to S_{18}$	$\overline{t}_{4\_18}$	20
5	$t_{\text{AccountPolice}}$	Среднее время блокирования смены учетных записей контроллера домена	$S_5 \to S_{18}$	$\overline{t}_{5\_18}$	13
6	t_{HASH}	Среднее время защиты от получения хэш-значений паролей из памяти	$S_7 \to S_5$	$\overline{t}_{7\_5}$	5
7	t_{CMD}	Среднее время защиты от запуска командной консоли	$S_9 \to S_7$	$\overline{t}_{9\_7}$	10
8	t_{Search}	Среднее время защиты от использования техники «*Remote System Discovery*»	$S_{12} \to S_{18}$	$\overline{t}_{12\_18}$	30
9	t_{Copy}	Среднее время защиты от несанкционированного копирования файлов «*Remote File Copy*»	$S_{15} \to S_{18}$	$\overline{t}_{15\_18}$	20
10	t_{Power}	Среднее время защиты от использования техники «*Endpoint Denial of Service*»	$S_{17} \to S_{18}$	$\overline{t}_{17\_18}$	10

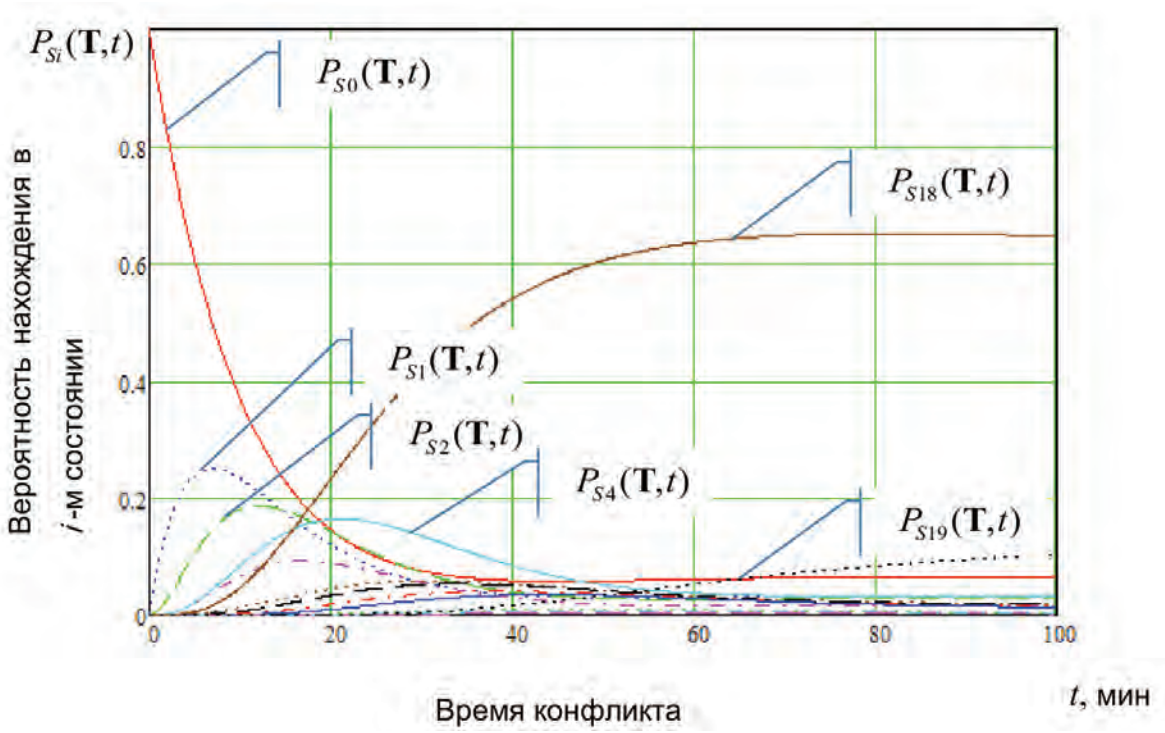

Рис. 2. Зависимость вероятности нахождения в различных состояниях графа от времени для типовых значений временных характеристик действий нарушителя и системы безопасности

порядка – метод Адамса, реализованный в среде MathCad. С применением численной реализации данного метода можно вычислить значения вероятностей во всех исследуемых состояниях в зависимости от времени t.

При оценке эффективности системы безопасности объекта КИИ в качестве показателя эффективности мер защиты от реализации компьютерной атаки, эксплуатирующей уязвимость Zerologon, используем отношение вероятностей нахождения в состояниях S_{18} и S_{19}, имеющих трактовку (см. таблицу 1): «Срабатывание системы безопасности и блокирование действий нарушителя в ходе атаки» и «Успешное завершение атаки»,

$$W(\mathbf{T},t)=\frac{P_{S18}(\mathbf{T},t)}{P_{S19}(\mathbf{T},t)}\quad , \qquad (3)$$

где $P_{S18}(\mathbf{T},t)$ – вероятность срабатывания системы безопасности и блокирования действий нарушителя в ходе атаки, $P_{S19}(\mathbf{T},t)$ – вероятность успешного завершения атаки ко времени t при заданных значениях множеств параметров $\mathbf{T}$, приведенных далее.

С учетом введенного показателя проведем исследование конфликтного взаимодействия системы безопасности и нарушителя на примере реализации компьютерной атаки, эксплуатирующей уязвимость Zerologon, в типовой информационной инфраструктуре, включающей корпоративную ЛВС с доменной архитектурой и автоматизированную систему управления неким технологическим процессом. Условимся считать, что в данной информационной инфраструктуре создана система безопасности объекта КИИ, основанная на применении мер защиты информации, временные характеристики которых, приведены в таблице 3. В этой таблица содержатся значения временных характеристик средств защиты, формализуемых соответствующими переходами графа, приведённого на рис. 1 и, физический смысл которых описан ранее в таблице 2.

Для типовых заданных значений множества параметров мер защиты $\mathbf{T}$, приведенных в столбце 6 таблицы 2 при численном решении методом Адамса в среде Mathcad системы (2) получены зависимости вероятностей нахождения в различных состояниях моделируемой системы $P_{Si}(\mathbf{T},t)$, где $\mathbf{T}=\mathbf{T}^{ЗИ}\bigcup\mathbf{T}^{наруш}$, $\mathbf{T}$ - множества значений временных параметров, характеризующих систему безопасности, $\mathbf{T}^{наруш}$ — множества значений временных параметров, характеризующих нарушителя. Будем считать, что варьируемыми параметрами в модели являются временные показатели мер защиты информации $\mathbf{T}$ из таблицы 3, а временные параметры нарушителя, взятые из таблицы 2, $\mathbf{T}^{наруш}=\{\overline{t}_{1\_2}, \overline{t}_{2\_3}, \overline{t}_{3\_4}, \overline{t}_{3\_18}, \overline{t}_{4\_5}, \overline{t}_{5\_6}, \overline{t}_{6\_5}, \overline{t}_{6\_7}, \overline{t}_{7\_9}, \overline{t}_{9\_12}, \overline{t}_{9\_18}, \overline{t}_{12\_15}, \overline{t}_{12\_17}, \overline{t}_{15\_19}, \overline{t}_{17\_19}, \overline{t}_{18\_0}\}$ определяются его квалификацией и задаются как исходные данные.

Наибольший интерес для исследования представляет начальная фаза конфликта, когда многие процессы находятся в переходных режимах. Вероятности нахождения в соответствующем i-м состоянии $P_{Si}(\mathbf{T},t)$ в начале конфликта $t=[1,100]$ приведены на рис. 2. Экстремальный характер кривых позволяет судить о возможности оптимизации параметров системы безопасности объектов КИИ.

Введенный ранее обобщенный показатель эффективности системы безопасности (8) зависит от значе-

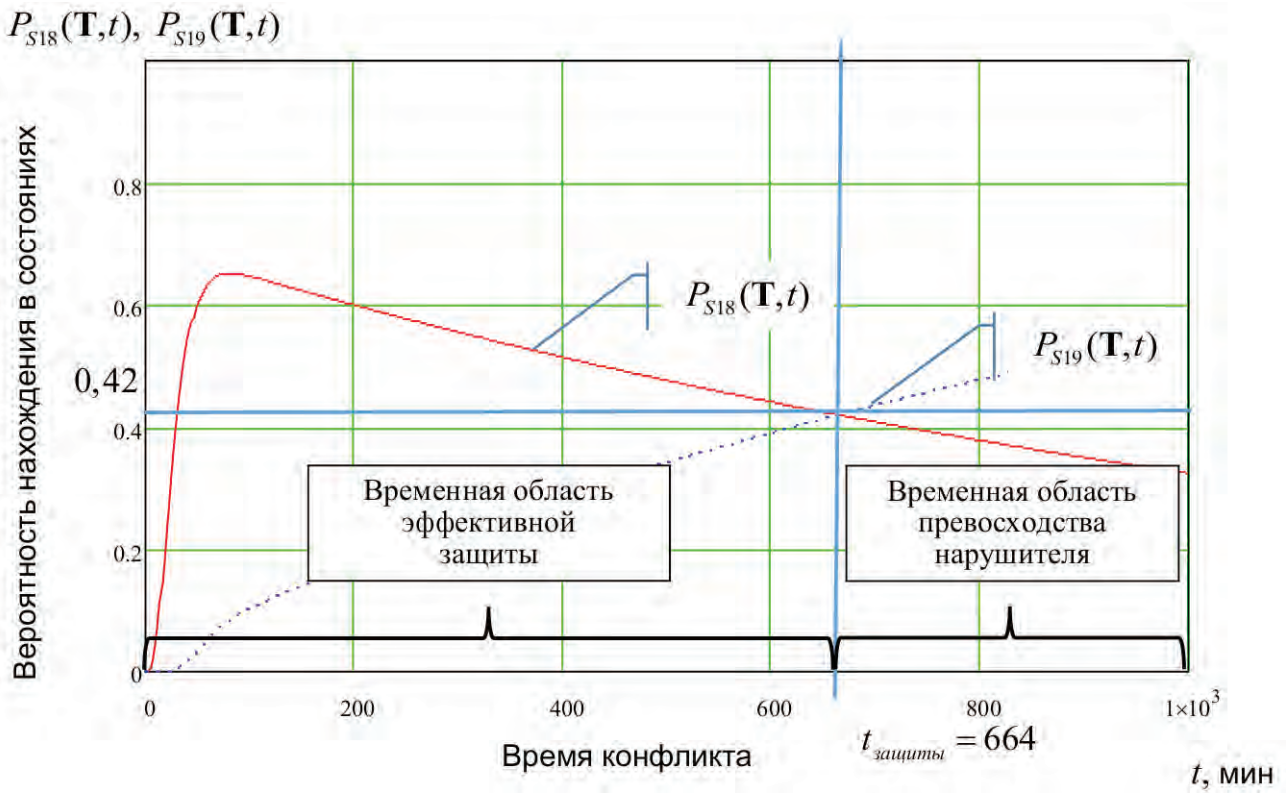

Рис.3. Значения вероятности нахождения в выигрышном и проигрышном состоянии от времени

ний вероятностей срабатывания системы безопасности и блокирования действий нарушителя в ходе атаки $P_{S18}(\mathbf{T},t)$ и успешного завершения атаки $P_{S19}(\mathbf{T},t)$. По сути процесса, эти состояния в итоге определяют выигрыш и проигрыш системы безопасности в конфликтном взаимодействии с нарушителем.

Интересующие нас зависимости вероятности нахождения в выигрышном $P_{S18}(\mathbf{T},t)$ и проигрышном $P_{S19}(\mathbf{T},t)$ состояниях от времени конфликта t на более длительном интервале исследования приведены на рис. 3. Этот рисунок наглядно показывает, что, решая уравнение

$$P_{S18}(\mathbf{T},t) = P_{S19}(\mathbf{T},t), \quad (4)$$

для типовых значений временных характеристик действий нарушителя и системы безопасности $\mathbf{T}$ можно определить момент времени, до которого значение вероятности нахождения в выигрышном состоянии $P_{S18}(\mathbf{T},t)$ будет больше значения вероятности нахождения в проигрышном состоянии $P_{S19}(\mathbf{T},t)$. Этот момент времени является границей между временной областью эффективной защиты, определяющий длительность выигрыша системы безопасности, и временной областью превосходства нарушителя, определяющий интервал времени, когда вероятность успешного завершения атаки будет больше чем вероятность срабатывания системы безопасности и блокирования действий нарушителя в ходе атаки.

Для значений параметров $\mathbf{T}$ характеристик мер защиты информации, приведенных в таблице 3, результат решения уравнения (4) показывает, что в течение 664 минут с момента начала атаки система будет обеспечивать защиту с вероятностью $P_{S18}(\mathbf{T},t)$ не ниже 0,42. При этом конфликтно-определяемая вероятность успешного завершения атаки $P_{S19}(\mathbf{T},t)$ будет значительно ниже. Превышение значения вероятности $P_{S18}(\mathbf{T},t)$ значения вероятности $P_{S19}(\mathbf{T},t)$ говорит о нахождении процесса во временной области эффективной защиты и действенности, входящих в систему безопасности объекта КИИ, мер защиты информации в момент времени $t = 664$ мин.

Следует отметить, что аналогичные временные значения параметров $\mathbf{T}$ можно получить, решая уравнение (3) по параметру t в виде

$$W(\mathbf{T},t) = \frac{P_{S18}(\mathbf{T},t)}{P_{S19}(\mathbf{T},t)} = 1. \quad (5)$$

Проведем исследование системы безопасности объекта КИИ в условиях воздействия компьютерных атак, эксплуатирующих уязвимость Zerologon, для трех различных наборов мер защиты, характеризуемых временными значениями $\mathbf{T}1, \mathbf{T}2, \mathbf{T}3$. Набор временных значений параметров мер защиты от реализации компьютерной атаки $\mathbf{T}1$ представляет собой набор типовых значений временных характеристик мер защиты информации, приведенный в таблице 3. В наборе значений $\mathbf{T}2$ ухудшены характеристики средств защиты и увеличено среднее время срабатывания меры защиты от сниффинга $t_{\text{WireShark}}$ с 8 до 15 минут.

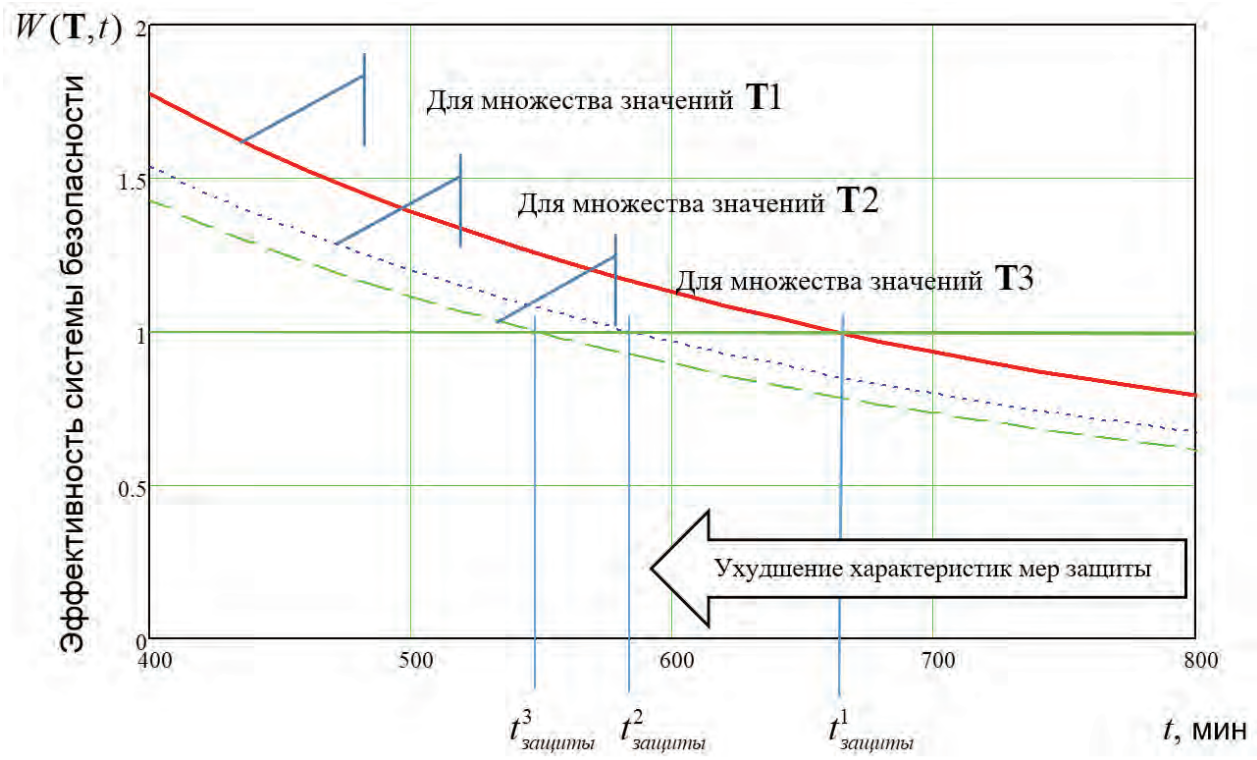

Рис. 4. Функция эффективности системы безопасности для различных наборов значений временных параметров средств защиты информации $\mathbf{T}$

В наборе значений $\mathbf{T}3$ в отличие от $\mathbf{T}1$ увеличено среднее время защиты от получения хэш-значений паролей из памяти t_{HASH} с 10 до 15 минут. Это может быть достигнуто за счет более оперативного обнаружения средств сниффинга путем обнаружения сетевых интерфейсов, работающих в promiscous-режиме, контроля над процессами и приложениями, присутствующими на серверах или узлах, с помощью системы обнаружения проникновений или обнаружений специфичных пакетов в трафике.

В свою очередь, набор мер, характеризуемых временными параметрами $\mathbf{T}1$, лучше чем набор мер, характеризуемых временными параметрами $\mathbf{T}3$, за счет использования системы более оперативного сигнатурного анализа сетевого трафика, исполнения правил для сетевых соединений, ведения черных и белых списков приложений. Т.е. набор мер, характеризуемых временными параметрами $\mathbf{T}1$, лучше чем набор мер, характеризуемых временными параметрами $\mathbf{T}2$ и набор мер $\mathbf{T}1$, лучше чем набор мер $\mathbf{T}3$.

Результат решения уравнения (5) для различных наборов временных значений параметров мер защиты от реализации компьютерной атаки $\mathbf{T} = \{\mathbf{T}1, \mathbf{T}2, \mathbf{T}3\}$ в виде графиков приведен на рис. 4. Как видно из рисунка, последовательное ухудшение временных параметров мер защиты по двум показателям $\mathbf{T}2$ и $\mathbf{T}3$ приводит к снижению времени защиты $t^1_{защиты} > t^2_{защиты} > t^3_{защиты}$. Как отмечалось ранее, значение этого времени определяет длительность эффективного функционирования системы безопасности и как, следствие, время устойчивого функционирования КИИ в условиях целенаправленных компьютерных атак, эксплуатирующей уязвимость Zerologon, с $t^1_{защиты}$ =664 (для набора временных параметров $\mathbf{T}1$) до $t^2_{защиты}$ =584 (для набора временных параметров $\mathbf{T}2$) и $t^3_{защиты}$ =548 (для набора временных параметров $\mathbf{T}3$) минут.

Анализ смещения влево при ухудшении параметров защиты значений времени защиты $t_{защиты}$, показанного на рис. 4, позволяет сделать вывод, что многопараметрическая функция эффективности мер защиты от компьютерной атаки, эксплуатирующей уязвимость Zerologon, является монотонно убывающей во времени функцией. Это говорит о том, что улучшение временных характеристик мер защиты (повышения оперативности) увеличивает время эффективной защиты $t_{защиты}$. Но, поскольку, снижение времени реакции мер защиты (повышение оперативности) имеет свои технологические пределы, то можно сделать вывод, что граница параметрической области значений $W(\mathbf{T},t)$ 1 по времени защиты t снизу будет ограничена нижними временными значениями вводимых ограничений, характеризующих меры защиты t_{DHCP}, $t_{\text{WireShark}}$, t_{SMB}, $t_{\text{Zerologon}}$, $t_{\text{AccountPolice}}$, t_{HASH}, t_{CMD}, t_{Search}, t_{Copy}, t_{Power}.

Проведем обоснование рациональных значений временных параметров системы безопасности объекта КИИ. В соответствии с (3) превышение показателя эффективности мер защиты от реализации компьютерной атаки $W(\mathbf{T},t)$ единичного значения говорит об эффективности системы безопасности объекта КИИ в момент времени t. Тогда для вводимых различных наборов значений $\mathbf{T}1, \mathbf{T}2, \mathbf{T}3$, характеризующих технические и вероятностно-временные характеристики

системы безопасности и инструментария нарушителя, можно выявить предельные для заданных ограничений моменты времени t_1, t_2 и t_3 гарантированного обеспечения защиты от компьютерных атак, эксплуатирующих уязвимость Zerologon, и как следствие устойчивого функционирования КИИ.

Это предполагает возможность превентивного управления ресурсами защиты путем снижения времени реагирования и реализации мер защиты на различных этапах атаки. Превентивность управления ресурсами защиты базируется на выборе на этапе разработки системы безопасности таких мер защиты информации и задании значений частных параметров множеств $\mathbf{T} \in \mathbf{T}$ с учетом ограничений, обеспечивающих эффективное функционирование системы безопасности в течение заданного времени. Выбор рациональных (оптимальных по критерию максимизации времени защиты $t_{защиты}$) средств защиты можно представить как результат решения задачи поиска переменных, являющихся аргументами функции эффективности системы безопасности объекта КИИ $W(\mathbf{T},t)$, максимизирующих время эффективного функционирования системы безопасности t в виде:

$$\max_{\mathbf{T}^{\mathcal{M}} \in \mathbf{T}} \arg_{t} (W(\mathbf{T},t) = 1), \quad (6)$$

где $\mathbf{T}$ – временные показатели мер защиты информации, характеризующие эффективность системы безопасности.

Полученные значения определяют технические требования по оперативности реагирования на инциденты компьютерной безопасности на различных этапах компьютерной атаки.

Результаты решения нелинейной задачи (6) методом сопряженных градиентов в среде Mathcad для заданных значений временных ограничений приведены в таблице 4.

Графики зависимости функции эффективности системы безопасности от времени для типовых (см. таблицу 3) $\mathbf{T}1$ и оптимальных (см. таблицу 4) значений параметров защиты $\mathbf{T}^*$ приведены на рис. 5. На нем показан рост времени устойчивого функционирования КИИ с 664 до 11328 мин (189 ч) при реализации рациональных средств защиты.

Получаемые при расчетах значения функции эффективности системы безопасности являются результатом вычисления функции, зависящей от 25 параметров, среди которых 10 определяют временные характеристики системы безопасности объекта КИИ. Это позволяет обосновать требования к системе безопасности объекта КИИ по оперативности для каждого этапа и в целом. Результаты расчетов по двум параметрам $t_{\text{WireShark}}$ и t_{SMB} приведены на рис. 6.

Как видно из рис. 6, максимальное значение времени эффективного функционирования системы безопасности в условиях проведения атак, эксплуатирующих уязвимость Zerologon, определяется оперативно-

Таблица 4

Значения временных параметров системы безопасности, максимизирующих значение времени защиты $t_{защиты}$

Обозначение	Характеристика	Ограничения	Оптимальное значение, мин
t_{DHCP}	Среднее время срабатывания меры защиты от подключения стороннего DHCP-клиента	$5 \le t_{DHCP} < 10$	5
$t_{\text{WireShark}}$	Среднее время срабатывания меры защиты от сниффинга	$10 \le t_{\text{WireShark}} < 30$	10
t_{SMB}	Среднее время срабатывания меры защиты от сканирования SMB ресурсов	$5 \le t_{\text{SMB}} < 15$	5
$t_{\text{Zerologon}}$	Среднее время применения патча и рекомендаций Microsoft по удалению уязвимости	$5 \le t_{\text{Zerologon}} < 10$	5
$t_{\text{AccountPolice}}$	Среднее время блокирования смены учетных записей контроллера домена	$5 \le t_{\text{AccountPolice}} < 10$	5
t_{HASH}	Среднее время защиты от получения хэш-значений паролей из памяти	$10 \le t_{\text{HASH}} < 30$	10
t_{CMD}	Среднее время защиты от запуска командной консоли	$5 \le t_{\text{CMD}} < 10$	5
t_{Search}	Среднее время защиты от использования техник RemoteSystemDiscovery	$10 \le t_{\text{Search}} < 50$	10
t_{Copy}	Среднее время защиты от несанкционированного копирования файлов RemoteFileCopy	$5 \le t_{\text{Copy}} < 10$	5
t_{Power}	Среднее время защиты от использования техник EndpointDenialofService	$5 \le t_{\text{Power}} < 10$	5

DOI:10.21681/2311-3456-2021-6-47-61

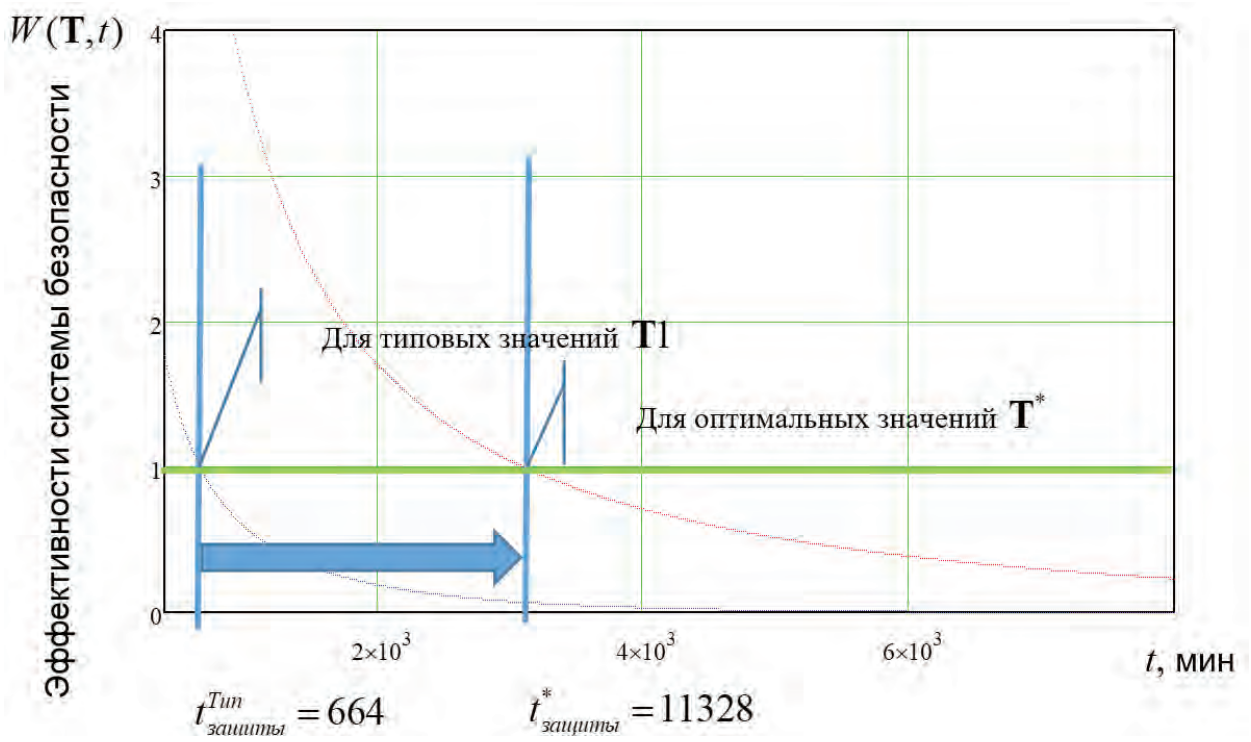

Рис. 5. Значение функции эффективности системы безопасности для типовых и оптимальных значений параметров защиты

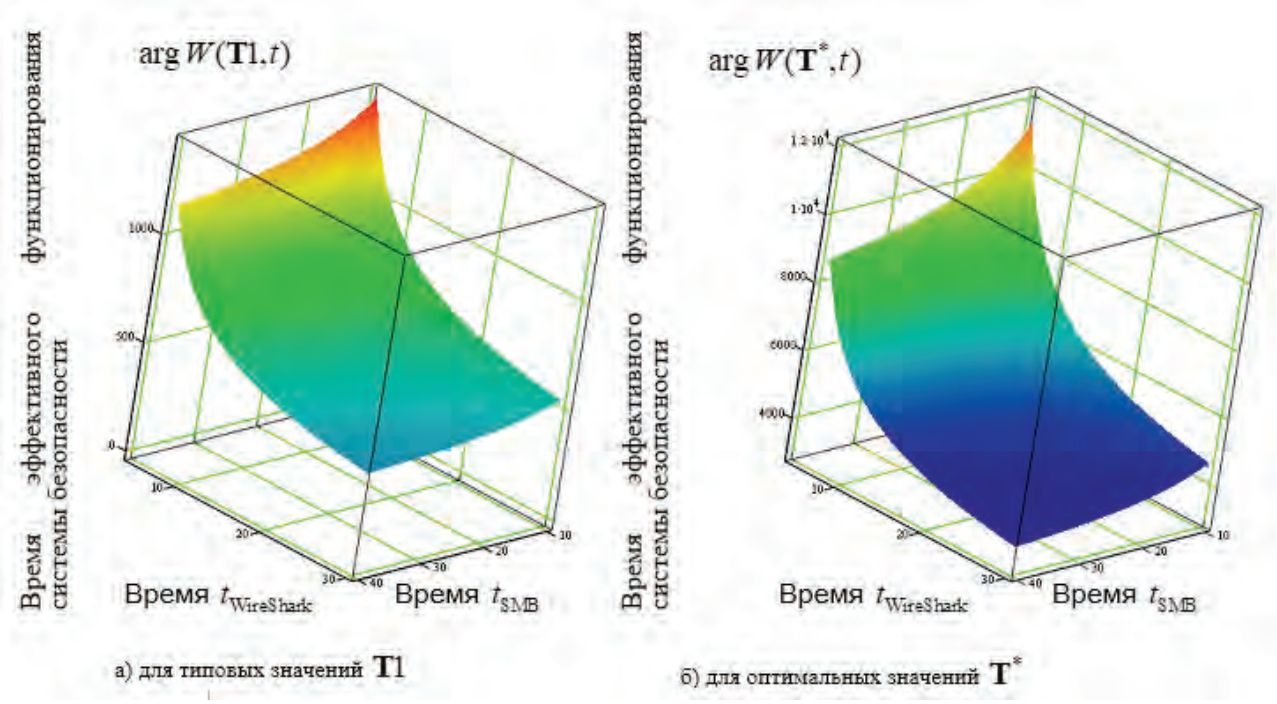

Рис. 6. Поверхность зависимости времени эффективного функционирования системы безопасности $t_{защиты}$ для типовых и оптимальных значений параметров защиты

стью (быстродействием) реагирования на те или иные инциденты компьютерной безопасности. Например, снижение времени реагирования на выявление, анализ и принятие мер по предотвращению повторного пассивного сбора (прослушивания) информации о подключенных к сети устройствах $t_{\text{WireShark}}$ или направленного сканирования при помощи специализированного программного обеспечения подключенных к сети устройств с целью получения конфигурационной информации компонентов систем и сетей t_{SMB} с 30 до 10 минут позволяет существенно продлить время эффективного функционирования системы безопасности.

Подобные выводы можно сделать и в отношении остальных временных характеристик системы безопасности объекта КИИ.

Выводы

Таким образом, в условиях возрастания угроз реализации компьютерных атак против значимых объектов КИИ актуальной задачей является разработка простых и адекватных математических моделей, позволяющих протестировать и оценить эффективность системы безопасности в ходе ее проектирования. Применение теории марковских процессов с дискретными состояниями и непрерывным временем позволяет достаточно точно формализовать процесс компьютерной атаки. Применение численных методов решения систем однородных дифференциальных уравнений, реализованных в среде проведения вычислительных расчетов Mathcad, позволило не только получить графические зависимости вероятностей нахождения в том или ином состоянии моделируемой системы, но и ввести новый функциональный показатель эффективности средств защиты от реализации компьютерной атаки $W(\mathbf{T},t)$. Введенный количественный показатель эффективности позволил наглядно продемонстрировать эффективность обоснованных временных параметров системы безопасности, максимизирующих время эффективного функционирования системы безопасности значимого объекта КИИ при проведении в отношении ее компьютерных атак. Рекомендуемые временные параметры рациональных средств защиты на различных этапах компьютерной атаки, эксплуатирующей уязвимость Zerologon, позволяют обеспечить безопасность и повысить время устойчивого функционирования критической информационной инфраструктуры с 11 до 189 часов.

Литература

1. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Штучний інтелект. 2008. № 4. С. 253-264.
2. Шелухин О.И. Моделирование информационных систем: учебное пособие для вузов. 2-е изд. М.: Горячая линия–Телеком, 2012. 516 с.
3. Котенко Д.И., Котенко И.В., Саенко И.Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. № 3(22). С. 5-30.
4. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 3-4 (129-130). С. 58-65.
5. Андреещев И.А., Будников С.А., Гладков А.В. Полумарковская модель оценки конфликтной устойчивости информационной инфраструктуры // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 1. С. 10-17.
6. Котенко Д.И., Котенко И.В., Саенко И.Б. Моделирование атак в больших компьютерных сетях // Технические науки - от теории к практике. 2013. № 17-1. С. 12-16.
7. Тумоян Е.П. Метод моделирования компьютерных атак на основе вероятностных автоматов // Известия ЮФУ. Технические науки. 2008. № 8 (85). С. 120-126.
8. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Воронеж: Кварта, 2015. 440 с.
9. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «Phishing» на локальную компьютерную сеть // Вопросы кибербезопасности. 2021. № 2(42). С. 17-25. DOI: 10.21681/2311-3456-2021-2-17-25.
10. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36. DOI: 10.18522/2311-3103-2016-8-2736.
11. Язов Ю.К., Анищенко А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. Монография. Воронеж: Кварта, 2020. 173 с.
12. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М.: Высшая школа, 2000. 383 с.
13. Фомичева С.Г., Жемелев Г.А. Моделирование эксплуатации уязвимости Zerologon // Завалишинские чтения'21: XVI Международная конференция по электромеханике и робототехнике, Санкт-Петербург, 15–18 апреля 2021 года. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2021. С. 334-341.
14. Вентцель Е.С. Исследование операций. М.: Советское радио, 1972. 552 с.
15. Охорзин В.А. Оптимизация экономических систем. Примеры и алгоритмы в среде Mathcad. М.: Финансы и статистика, 2005. 144 с.

MODELING OF APT-ATTACKS EXPLOITING THE ZEROLOGON VULNERABILITY

Budnikov S.A.[9], Butrik E.E.[10], Soloviev S.V.[11]

Purpose: *the need to assess the effectiveness of the security systems for significant objects of critical information infrastructure determines the need to develop simple and adequate mathematical models of computer attacks. The use of mathematical modeling methods in the design of security system of significant object allows without significant cost and impact on the functioning of the object to justify the requirements to the system as a whole or its individual parts. The purpose of the present paper is to develop a model of the process of multistage targeted computer attack that exploits the Zerologon vulnerability, based on the representation of the attack by a Markov random process with discrete states and continuous time.*

Methods: *methods of Markov process theory, probability theory, computational mathematics and graph theory are used in the model to formalize the attack.*

Novelty: *application of methods of computational mathematics for functional analysis of the results of Kolmogorov's system of equations allows to solve the problem of maximizing the time of stable operation of critical information infrastructure during computer attacks against it, using the known methods of analysis of continuous functions.*

Result: *formulated a general statement of the problem of modeling the process of a multistage targeted computer attack using a system of Kolmogorov equations, describing the probabilities of being in conflict states of the security system with the intruder. By the Adams method implemented in Mathcad environment, numerical solutions depending on time were obtained. We introduce a security system performance index as a ratio of probability of triggering the security system and blocking* intruder's actions during the attack to the probability of successful completion of the attack. We give an example of research of computer attack realization in a typical information infrastructure, including a corporate network with domain architecture and an automated control system of some technological process. 1 For the considered example defined the optimal values of time parameters of security system. When implementing protective measures with reasonable probabilistic-time characteristics proved an increase in time of stable operation of critical information infrastructure from 11 to 189 hours.

Keywords: *significant object, computer attack, critical information infrastructure, Markov processes, security system.*

References

1. Maslova N.A. Metody` ocenki e`ffektivnosti sistem zashhity` informacionny`x sistem // Shtuchnij intelekt. 2008. № 4. S. 253-264.
2. Sheluxin O.I. Modelirovanie informacionny`x sistem: uchebnoe posobie dlya vuzov. 2-e izd. M.: Goryachaya liniya–Telekom, 2012. 516 s.
3. Kotenko D.I., Kotenko I.V., Saenko I.B. Metody` i sredstva modelirovaniya atak v bol`shix komp`yuterny`x setyax: sostoyanie problemy' // Trudy` SPIIRAN. 2012. № 3(22). S. 5-30.
4. Kocynyak M.A., Lauta O.S., Ivanov D.A., Lukina O.M. Model` vozdejstviya targetirovannoj kiberneticheskoj ataki na informacionno-telekommunikacionnuyu set` // Voprosy` oboronnoj texniki. Seriya 16: Texnicheskie sredstva protivodejstviya terrorizmu. 2019. № 3-4 (129-130). S. 58-65.
5. Andreeshhev I.A., Budnikov S.A., Gladkov A.V. Polumarkovskaya model` ocenki konfliktnoj ustojchivosti informacionnoj infrastruktury` // Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemny`j analiz i informacionny`e texnologii. 2017. № 1. S. 10-17.
6. Kotenko D.I., Kotenko I.V., Saenko I.B. Modelirovanie atak v bol`shix komp`yuterny`x setyax // Texnicheskie nauki - ot teorii k praktike. 2013. № 17-1. S. 12-16.
7. Tumoyan E.P. Metod modelirovaniya komp`yuterny`x atak na osnove veroyatnostny`x avtomatov // Izvestiya YuFU. Texnicheskie nauki. 2008. № 8 (85). S. 120-126.
8. Yazov Yu.K., Solov`ev S.V. Zashhita informacii v informacionny`x sistemax ot nesankcionirovannogo dostupa. Voronezh: Kvarta, 2015. 440 s.
9. Dobry`shin M.M., Zakalkin P.V. Model` komp`yuternoj ataki tipa «Phishing» na lokal`nuyu komp`yuternuyu set` // Voprosy` kiberbezopasnosti. 2021. № 2(42). S. 17-25. DOI: 10.21681/2311-3456-2021-2-17-25.
10. Klimov S.M. Imitacionny`e modeli ispy`tanij kriticheski vazhny`x informacionny`x ob``ektov v usloviyax komp`yuterny`x atak // Izvestiya YuFU. Texnicheskie nauki. 2016. № 8 (181). S. 27-36. DOI: 10.18522/2311-3103-2016-8-2736.

9 Sergey Budnikov, Dr.Sc.. (of Tech.), Associate Professor, chief researcher of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». Voronezh, Russia. E-mail: buser@bk.ru.

10 Ekaterina Butrik, post-graduate student of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». Voronezh, Russia. E-mail: keit1991@list.ru.

11 Sergey Soloviev, Ph.D., Associate Professor, head of department of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». Voronezh, Russia. E-mail: sersol@mail.ru.

11. Yazov Yu.K., Anishhenko A.V. Seti Petri-Markova i ix primenenie dlya modelirovaniya processov realizacii ugroz bezopasnosti informacii v informacionny`x sistemax. Monografiya. Voronezh: Kvarta, 2020. 173 s.
12. Ventcel` E.S., Ovcharov L.A. Teoriya sluchajny`x processov i ee inzhenerny`e prilozheniya. M.: Vy`sshaya shkola, 2000. 383 s.
13. Fomicheva S.G., Zhemelev G.A. Modelirovanie e`kspluatacii uyazvimosti Zerologon // Zavalishinskie chteniya'21: XVI Mezhdunarodnaya konferenciya po e`lektromexanike i robototexnike, Sankt-Peterburg, 15–18 aprelya 2021 goda. Sankt-Peterburg: Sankt-Peterburgskij gosudarstvenny`j universitet ae`rokosmicheskogo priborostroeniya, 2021. S. 334-341.
14. Ventcel` E.S. Issledovanie operacij. M.: Sovetskoe radio, 1972. 552 s.
15. Oxorzin V.A. Optimizaciya e`konomicheskix sistem. Primery` i algoritmy` v srede Mathcad. M.: Finansy` i statistika, 2005. 144 s.