УДК 123.456.789

Подтверждение адекватности математической модели, описывающей динамику возможности реализации компьютерной атаки во времени

О. С. Макарова[1], С. В. Поршнев

Одной из актуальных проблем информационной безопасности на текущий момент является отсутствие единого подхода к прогнозированию компьютерных атак, что подтверждается как международными, так и российскими экспертами, а также практикой. В работе предложена математическая модель, описывающая динамику реализации компьютерной атаки (КА) во времени, построенная на базе теории диффузии инноваций (ТДИ). Приводится обоснование возможности использования ТДИ, описывается отличие киберпреступлений от иных видов преступлений. Адекватность предложенной модели подтверждается, в частности, натурным моделированием КА на ресурсы организации через интернет-сайт. Данные практических экспериментов подтверждают математическую модель, в частности, функцию вероятности возможности реализации КА во времени, т.е. изменение числа зараженных узлов во времени можно аппроксимировать с помощью s-образной кривой Перла–Рида или каскадной модели. Оптимальность данной аппроксимации доказывается методом наименьших квадратов.

Ключевые слова: компьютерная атака, кривые Перла–Рида, теория диффузии инноваций, динамика распространения компьютерной атака, натурное моделирование, компьютерная атака на ресурсы организации через интернет-сайт, аппроксимация.

1. Введение

Анализ действующей нормативно-правовой базы в области информационной безопасности (ИБ), соответствующих научных исследований, в том числе посвященных разработке методов расчета вероятности угроз на основе нормативных документов ФСТЭК России и ФСБ России, методов оценки рисков ИБ на базе международных стандартов, методов по оптимизации оценки рисков ИБ и прогнозированию уязвимостей, угроз ИБ и методов КА позволяют сделать обоснованный вывод об отсутствии единого метода прогнозирования наиболее вероятных векторов КА и соответствующих математических моделей. Это подтверждается:

- аналитическими отчетами российских специалистов (см. Паспорт федерального проекта «Информационная безопасность» [□]);
- аналитическими отчетами зарубежных специалистов («Отчет Всемирного экономического форума по глобальным рискам» [□]);
- результатами соревнований по кибербезопасности между командами атакующих, защитников и специалистов в области мониторинга ИБ (например, PHDays [3, 4]).

Проведение анализа динамики развития КА позволит определить возможности, вид и критерии развития КА, улучшив таким образом средства и методы выявления и предупреждения компьютерных преступлений.

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ).

2. Математическая модель, описывающая динамику возможности реализации компьютерной атаки во времени

Для разработки математической модели, описывающей динамику возможности реализации КА во времени, проведем анализ особенностей КА с точки зрения нарушителя (этапы и методы реализации КА) и факторов, определяющих динамику изменения возможности реализации КА.

При этом учтем, что компьютерные преступления, в отличие от правонарушений, являющихся предметом, изучаемым криминологией, требуют от нарушителя наличия специальных знаний, умений и навыков, а также возможности практически совершить КА. Рассмотрим подробнее умения и навыки нарушителя. Знания о методах КА нарушитель может приобрести в *DarkNet* – это области Интернета, в которые не может попасть обычный пользователь через поисковики *Google* или *Yandex*. Для доступа к *DarkNet* необходимо использовать программное обеспечение (ПО), обеспечивающее анонимное подключение, например, *The Onion Router*. Для большей конфиденциальности нарушители на форумах *DarkNet* используют технологию *Virtual Private Network*. Анализ форумов в *DarkNet* позволяет собрать информацию о стратегиях, тактиках и методах, которые используют и/или разрабатывают нарушители для реализации КА. Различные решения по сбору информации с форумов *DarkNet* рассматриваются в [5–9].

Таким образом, на подготовительном этапе проведения КА нарушитель стремится получить сведения о новых для него технологиях проведения КА, которые, следуя [10], являются синонимом понятия «инновация» (инновация – технологическая идея, метод или объект, являющийся новым для члена социальной системы). В этой связи можно предположить, что динамика КА может быть построена на основе положений и математических моделей ТДИ (здесь диффузия инноваций – это процесс, с помощью которого инновации распространяются по каналам передачи с течением времени среди членов социальной системы), развитых Э. Роджерсом [10], Ф. Бассом [11], Э. Мэнсфилдом [12] и Т. Хагерстрандом [**Ошибка! Источник ссылки не найден.**].

Напомним, что накопленные суммы приобретенных инноваций от времени описываются зависимостью $Y(t)$ вида:

$$Y(t) = \frac{1}{1+\alpha e^{-\beta t}}, \tag{1}$$

где α, β – параметры модели, называемых *s*-образными кривыми Перла–Рида.

Согласно исследованиям, проведенным в [**Ошибка! Источник ссылки не найден.**], инновация может также развиваться по каскадной модели, описываемой следующей формулой:

$$Y(t) = \begin{cases} \dfrac{1}{1+\alpha_1 e^{-\beta_1 (t-t_0)}}, \text{ если } t_0 \le t \le t_1, \\ \dfrac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \dfrac{1}{1+\alpha_2 e^{-\beta_2 (t-t_1)}}, \text{ если } t_1 \le t \le t_2, \\ \dots \\ \dfrac{1}{1+\alpha_1 e^{-\beta_1 (t_1-t_0)}} + \dfrac{1}{1+\alpha_2 e^{-\beta_2 (t_2-t_1)}} + \dots \quad \dfrac{1}{1+\alpha_n e^{-\beta_n (t-t_{n-1})}}, \text{ если } t_{n-1} \le t \le t_n, \end{cases} \tag{2}$$

где $[t_0, t_1]$ – длительность первого этапа развития инновации; если

$]t_1, t_2]$ – длительность второго этапа развития инновации;

…

$]t_{n-1}, t_n]$ – длительность *n*-го этапа внедрения инновации.

Корректность такого упрощения для новых прогрессивных технологий, к которым относятся информационные технологии (ИТ) и ИБ-технологии, была подтверждена Э. Мэнсфилдом [12].

Для подтверждения адекватности описанной математической модели, описывающей динамику развития КА, могут использоваться экспериментальные исследования КА на стенде.

3. Подтверждение адекватности математической модели динамики распространения компьютерной атаки с помощью натурного моделирования на ПАК «Ampire»

Для экспериментального подтверждения адекватности математических моделей, описывающих динамику развития КА, был использован программно-аппаратный комплекс (ПАК) обучения методам обнаружения, анализа и устранения последствий КА «Ampire» [14], разработанный компанией ОА «Перспективный мониторинг».

ПАК «Ampire» позволяет моделировать типовые и специализированные информационные системы (ИС), активировать векторы КА, характерные для внешнего и внутреннего нарушителей. Комплекс предоставляет пользователю специализированное ПО для обнаружения следов КА, а также инструменты для повышения уровня защищенности ИС, на которой проходит тренировка. Интерфейс ПАК «Ampire» представлен на рис. 1Рис. 1.

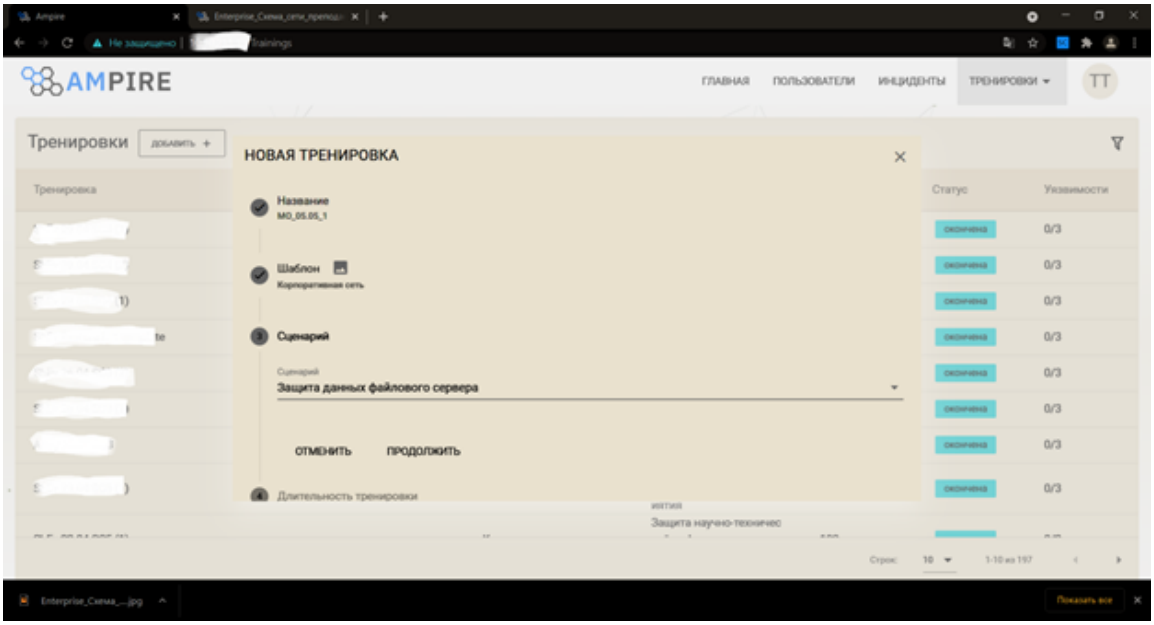

Рис. 1. Интерфейс ПАК «Ampire» в режиме задания сценария КА (новой тренировки)

В ПАК «Ampire» реализованы следующие функции:

- создание экземпляров КС на базе имеющихся шаблонов;
- управление пользователями, которые проходят обучение (создание профиля, распределение по группам, редактирование и удаление);
- управление виртуальными нарушителями (активация действий, остановка, выполнение отдельных шагов);
- создание тренировок, в которых объединяются экземпляры КС, пользователи и виртуальные нарушители;
- получение информации о ходе запущенных тренировок (количество и содержимое заведенных карточек инцидентов, статус по устранению имеющихся уязвимостей в экземплярах ИС, работоспособности инфраструктуры ПАК «Ampire»);

– взаимодействие между пользователями посредством встроенного мессенджера и системы тикетов;
– оценка качества работы обучаемых;
– вывод статистической информации из ПАК «Ampire» по результатам проведенных тренировок.

ПАК «Ampire» (Academic) включает в свой состав серверное оборудование, демонстрационное оборудование и ПО. Шаблоном ИС в ПАК «Ampire» является набор виртуальных машин (серверы, рабочие станции, сетевое оборудование и т.д.), которые моделируют работу типовой КС организации (например, предприятие топливно-энергетической сферы, кредитно-финансовой сферы, офис).

3.1. Методика проведения натурного моделирования компьютерной атаки

При проведении натурного моделирования динамики развития КА был реализован следующий сценарий целевой КА на инфраструктуру организации, схема которой представлена на рис. 2.

Внешний нарушитель находит в сети интернет-сайт организации и принимает решение о проведении КА на него с целью получения доступа к внутренним ресурсам. Обнаружив и проэксплуатировав уязвимость на интернет-сайте, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям организации инструмент для генерации отчетов. С помощью этого вектора нарушитель пытается получить доступ к рабочим машинам сотрудников. Главная цель КА – сделать дамп корпоративной базы данных (БД). Проводимая КА считалась идеальной, поэтому действия специалистов ИБ по обнаружению, блокировке нарушителя и устранению последствий КА не предполагались. Событие ИБ характеризовалось:

– временем реализации действия нарушителем;
– этапом КА в соответствие с *Cyber Kill Chain* [15, 16] (временной интервал, в течение которого было реализовано действие нарушителя);
– описанием действия нарушителя;
– результатом, достигнутым нарушителем в результате реализованной КА.

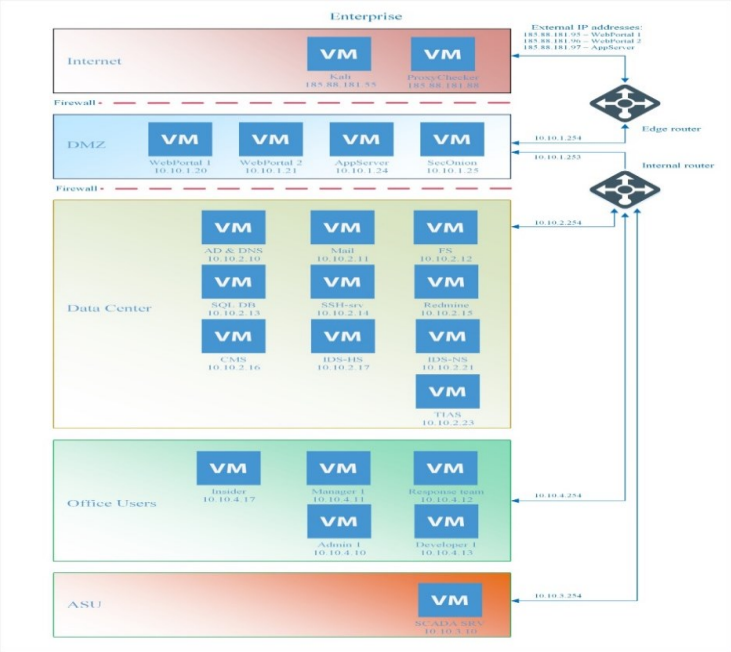

Рис. 2. Схема стенда организации, на которой реализуется сценарий КА

Описанный сценарий КА был реализован в виде скрипта, имитирующего действия потенциального нарушителя. Минимальная задержка между реализацией различных методов КА составляла 5 минут. Логирование всех действий нарушителя осуществлялось пользователем, имеющим статус «преподаватель».

Далее проводился анализ файла, содержащего информацию о событиях ИБ, с целью вычисления значений зависимости относительного числа «зараженных узлов» от времени. При этом было принято во внимание, что целью КА является не нарушение доступности, но нарушение конфиденциальности, т.е. получение дополнительной информации об «узле». В этой связи получение доступа к любому из 7 уровней модели OSI соответствующего автоматизированного рабочего места рассматривалось как событие доступа КА, состоящее в получении доступа нарушителя к узлу КС. Отметим, что обнаруженная уязвимость и ее эксплуатация рассматривались как дополнительная информация, которая учитывалась при расчете количества «зараженных узлов».

3.2. Анализ результатов натурного моделирования динамики развития компьютерной атаки

Журнал событий ИБ, сформированный в ходе проведения натурного моделирования КА, представлен в табл. 1. Здесь зараженным узлом считается узел, на котором злоумышленник получил доступ к одному из уровней модели OSI виртуальных машин стенда. В том случае, когда зараженный узел КС далее дополнительно применяет новый метод реализации КА на следующий узел КС, число зараженных узлов увеличивается на 0.5 (так как при выборе нового метода проведения КА с вероятностью 0.5 данная КА будет либо успешной, либо нет).

Таблица 1. Журнал зарегистрированных событий ИБ в ходе натурного моделирования КА

№ события	Время реализации КА	Этап КА	Описание этапа КА	Действие нарушителя	Количество «зараженных узлов», нарастающим итогом
1	7:37:55	0	Подготовка к проведению КА	Подготовка к проведению КА	0
2	7:38:25	0	Подготовка к проведению КА	Подготовка к проведению КА	0
3	7:38:55	1	Сканирование внешней сети организации, поиск открытого порта 80	Начало КА на сеть 185.88.181.0/24	0.5
4	7:40:01	1	Сканирование внешней сети организации, поиск открытого порта 81	Обнаружен веб-сервер (185.88.181.88, 185.88.181.95, 185.88.181.96, 185.88.181.97)	4.5
5	7:40:31	1	Сканирование внешней сети организации, поиск открытого порта 82	Не удалось подключиться к 185.88.181.88	4.5
6	7:42:12	1	Сканирование внешней сети организации, поиск открытого порта 83	Не удалось подключиться к 185.88.181.97	4.5
7	7:42:22	2	Эксплуатация уязвимости на веб-ресурсе и получение доступа к *DMZ*	Попытка эксплуатации уязвимости на 185.88.181.96	5

№ события	Время реализации КА	Этап КА	Описание этапа КА	Действие нарушителя	Количество «зараженных узлов», нарастающим итогом
8	7:42:33	2	Эксплуатация уязвимости на веб-ресурсе и получение доступа к *DMZ*	*WebShell* загружен, эксплуатация уязвимости прошла успешно	6
9	7:44:23	2	Подготовка полезной нагрузки, загрузка ее на веб-сервер	Подготовка полезной нагрузки	6.5
10	7:46:53	2	Подготовка полезной нагрузки, загрузка ее на веб-сервер	Жду запуска файла администратором	6.5
11	7:49:08	3	Сканирование сегмента внутренней сети в поисках сервисов	Начало сканирования внутренней сети	7
12	7:49:18	3	Сканирование сегмента внутренней сети в поисках сервисов	Сканирую подсеть 10.10.2.0/27	8
13	7:49:38	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.15	9
14	7:49:58	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.23	10
15	7:50:18	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.13	11
16	7:50:28	3	Сканирование сегмента внутренней сети в поисках сервисов	Обнаружен *ssh* по адресу 10.10.2.14	12
17	7:50:38	3	Сканирование сегмента внутренней сети в поисках сервисов	Сканирование подсети 10.10.2.0/27 завершено	12
18	7:51:38	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Начало перебора паролей к *ssh*-серверу	12,5
19	7:51:43	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.23	12.5
20	7:51:44	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Пароль к *ssh* не найден на 10.10.2.23, пробую следующий сервер *Medusa v*2.2	12.5

№ события	Время реализации КА	Этап КА	Описание этапа КА	Действие нарушителя	Количество «зараженных узлов», нарастающим итогом
21	7:51:45	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.13	12.5
22	7:53:49	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Пароль к *ssh*-серверу 10.10.2.13 успешно подобран *qwe123!@#*	13.5
23	7:53:54	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Перебор паролей на 10.10.2.14	13.5
24	7:54:45	4	Подбор пароля для подключения к *ssh*-серверу базы данных и получение доступа к файловой системе	Пароль к 10.10.2.14 успешно подобран *q123!@#*	14.5
25	7:54:45	4	Выполнение команды *history*, обнаружение пароля от базы данных	Выполнение команды *history*	16
26	7:54:46	4	Выполнение команды *history*, обнаружение пароля от базы данных	Выполнение команды *history* на *ssh*-серверах	17.5
27	7:54:54	4	Выполнение команды *history*, обнаружение пароля от базы данных	В выводе команды *history* на 10.10.2.14 отсутствуют данные для подключения	18.5
28	7:55:21	4	Выполнение команды *history*, обнаружение пароля от базы данных	Пароль к *mysql* найден *qwe123asd*	19.5
29	7:55:23	4	Выполнение команды history, обнаружение пароля от базы данных	Бот успешно похитил секреты вашей организации	19.5
30	7:58:24	4	Цели КА достигнуты	Заражено максимально возможное число узлов	19.5

Для удобства дальнейшего анализа моменты времени, указанные в табл. 1, пересчитывались в новые значения временной сетки, у которой за начало отсчета выбран момент времени 7:37:55, за единицу отсчета – секунды (см. табл. 2).

Таблица 2. Соответствие между моментами времени, в которые произошли события в ходе проведения КА, в абсолютном времени и выбранной системе измерения времени

№ события	Абсолютное время	Модифицированная временная шкала	№ события	Абсолютное время	Модифицированная временная шкала
1	7:37:55	0	16	7:50:28	753
2	7:38:25	30	17	7:50:38	763
3	7:38:55	60	18	7:51:38	823
4	7:40:01	126	19	7:51:43	828
5	7:40:31	156	20	7:51:44	829
6	7:42:12	257	21	7:51:45	830
7	7:42:22	267	22	7:53:49	954
8	7:42:33	278	23	7:53:54	959
9	7:44:23	388	24	7:54:45	1010
10	7:46:53	538	25	7:54:46	1011
11	7:49:08	673	26	7:54:47	1012
12	7:49:18	683	27	7:54:54	1019
13	7:49:38	703	28	7:55:21	1046
14	7:49:58	723	29	7:55:23	1048
15	7:50:18	743	30	7:58:23	1228

Зависимость относительного числа зараженных узлов КС от времени (отношение числа зараженных узлов к общему числу узлов), характеризующая, как показано в математической модели, динамику изменения КА, вычисленная на основе данных, представленных в табл. 1, табл. 2, представлена на рис. 3.

3.3. Результаты аппроксимации экспериментальной зависимости числа зараженных узлов от времени

Визуальный анализ зависимости числа зараженных узлов от времени, представленной на рис. 3, позволяет предположить, что данная зависимость может быть аппроксимирована функцией вида (2), которая представляет собой набор s-образных кривых Перла–Рида, заданных на последовательных интервалах:

1-ый интервал, начало в 7 часов 36 минут 55 секунд, окончание в 7 часов 40 минут 22 секунды;

2-й интервал, начало в 7 часов 40 минут 31 секунду, окончание в 7 часов 46 минут 53 секунды;

3-й интервал, начало в 7 часов 46 минут 53 секунды, окончание в 7 часов 51 минуту 43 секунды;

4-й интервал, начало в 7 часов 51 минуту 43 секунды, окончание 7 часов 58 минут 23 секунды.

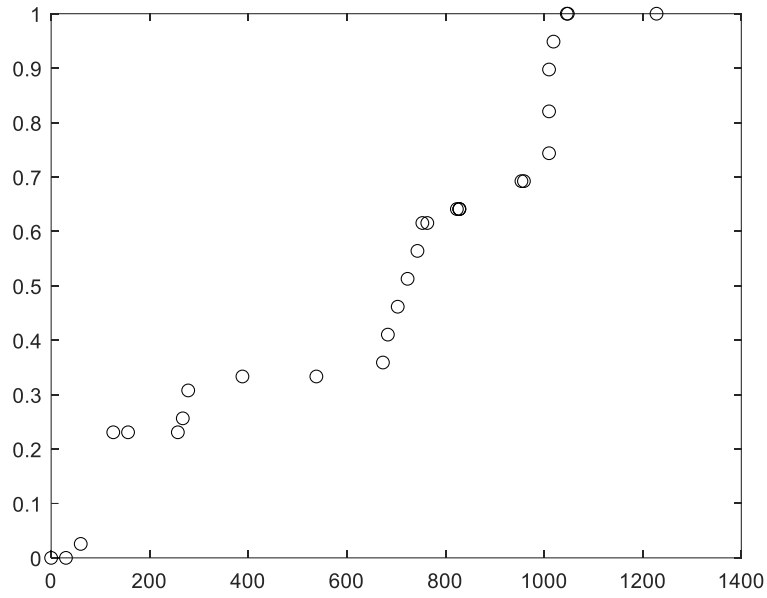

Рис. 3. Зависимость относительного числа зараженных узлов КС от времени при натурном моделировании КА

Далее на каждом из выбранных временных интервалов в соответствие с методом наименьших квадратов были вычислены параметры s-образных кривых Перла–Рида, аппроксимировавшийся на выбранных временных интервалах функциями

$$y_k(t) = \alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3 e^{-\alpha_4^{\langle k \rangle}(t - t_0^{\langle k \rangle})}}, \tag{3}$$

где $k = \overline{1,4}$ – номер интервала аппроксимации.

Значения коэффициентов аппроксимирующих функций $\alpha_j^{\langle k \rangle}$, $j = \overline{1,4}$ находились из условия:

$$\underset{\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}}{\arg} \min \left(\sum_{i=1}^{N^{\langle k \rangle}} \left(y_i - \left(\alpha_1^{\langle k \rangle} + \frac{\alpha_2^{\langle k \rangle}}{1 + \alpha_3^{\langle k \rangle} \exp\left(-\left(\alpha_4^{\langle k \rangle} (t_i - t_1) \right) \right)} \right) \right) \right)^2, \tag{4}$$

где $N^{\langle k \rangle}$ – число отсчетов аппроксимируемой зависимости, укладывающихся на *k*-ом интервале, с помощью функции пакета MATLAB fminsearch.m.

Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}$, удовлетворяющих (6), представлены в табл. 3. Также в табл. 3 приведены использованные начальные приближения значений этих коэффициентов.

Таблица 3. Значения коэффициентов аппроксимирующих функций $\alpha_1^{\langle k \rangle}, \alpha_2^{\langle k \rangle}, \alpha_3^{\langle k \rangle}, \alpha_4^{\langle k \rangle}$

k	Начальное приближение				Значения коэффиентов			
	$\alpha_1^{\langle k \rangle}$	$\alpha_2^{\langle k \rangle}$	$\alpha_3^{\langle k \rangle}$	$\alpha_4^{\langle k \rangle}$	$\alpha_1^{\langle k \rangle}$	$\alpha_2^{\langle k \rangle}$	$\alpha_3^{\langle k \rangle}$	$\alpha_4^{\langle k \rangle}$
1	0	0.1	1.0	200.0	–0.0076	0.2409	0.0658	216.6173
2	0.2308	0.1	1.0	400.0	0.2241	0.10925	0.1862	15.3182
3	0.3333	0.1	5.0	10.0	0.3237	0.33365	0.0353	466.8322
4	0.6410	0.1	1.0	40.0	0.6503	0.3720	0.0560	23712.73138

Результаты аппроксимации зависимости относительного числа зараженных узлов от времени представлены на рис. 4.

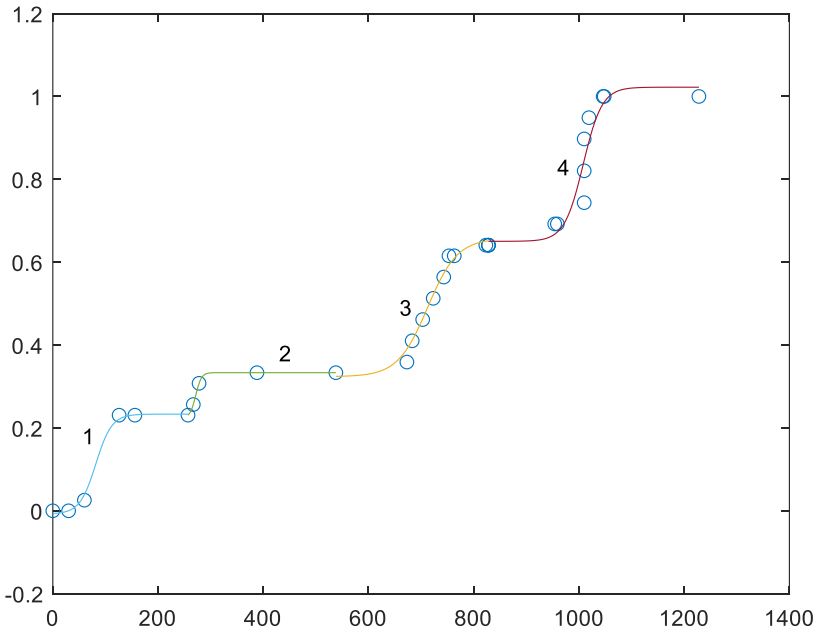

Рис. 4. Результаты аппроксимации зависимости количества зараженных узлов на каждом этапе натурного моделирования каскадной моделью s-образных кривых Перла–Рида

Из рис. 4 видно, что, действительно, динамика заражения узлов КС, которая в развиваемой нами модели эквивалентна динамике изменения вероятности реализации КА от времени на этапе прогнозирования, может быть описана с помощью каскадной математической модели (2).

4. Заключение

Обоснованы базовые принципы и подходы, на которых построена математическая модель, описывающая динамику изменения вектора КА во времени, с позиции нарушителя.

Оценка результатов практической апробации подтвердила, что вид функции изменения вектора КА соответствует предложенной математической модели. Вектор КА определяется характеристиками самой КА, в частности, экономичностью и рентабельностью реализации метода КА, наличием рекламы в *DarkNet* и данными межличностного взаимодействия нарушителей и апробации (совместимости с инфраструктурой атакуемых организаций, простотой реализации, наличием средств ЗИ и методов обнаружения КА).

Перспективы дальнейшей разработки темы исследования заключаются в:

– Определении значений параметров функции вероятности возможности реализации КА во времени.
– Автоматизации сбора и анализа информации из общедоступных источников информации о КА для прогнозирования векторов КА во времени с точки зрения нарушителя.

Литература

1. Паспорт федерального проекта «Информационная безопасность». Утвержден Правительственной комиссией по цифровому развитию, использованию информационных техноло-

гий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28 мая 2019 г. № 6.
2. The Global Risks Report 2018 // MARSH&McLENNAN COMPANIES. 2018. № 13. P. 80. [Электронный ресурс]. URL: https://www.marsh.com/us/insights/research/the-global-risks-report-2018.html (дата обращения: 27.04.2020).
3. Кибербитва на PHDays, или Как за 30 часов взломать городскую инфраструктуру. [Электронный ресурс]. URL: https://www.phdays.com/ru/press/news/kiberbitva-na-phdays-ili-kak-za-30-chasov-vzlomat-gorodskuyu-infrastrukturu/ (дата обращения: 27.04.2020).
4. PHDays: точно в девятку. [Электронный ресурс]. URL: https://www.phdays.com/ru/press/news/phdays-tochno-v-devyatku/ (дата обращения: 27.04.2020).
5. *Choi S.-K., Lee T., Kwak J.* Study on analysis of malicious code behavior information for predicting security threats in new environments // KSII Transactions on Internet and Information Systems. 2019. № 13 (3). P. 1611–1625. DOI: https://doi.org/10.3837/tiis.2019.03.028.
6. *Feng B., Li Q., Ji Y., Guo D., and Meng X.* Stopping the cyberattack in the early stage: assessing the security risks of social network users // Hindawi magazine. 2019. DOI: https://doi.org/10.1155/2019/3053418.
7. *Nalini M., Chakram A.* Digital risk management for data attacks against state evaluation // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2020. № 88. DOI: https://doi.org/10.35940/ijitee.I1130.0789S419.
8. *Deb A., Lerman K., and Ferrara E.* Predicting cyber events by leveraging hacker sentiment // Information. 2018. № 9 (11). P. 18. DOI: https://doi.org/10.3390/info9110280.
9. *Zenebe A., Shumba M., Carillo A., and Cuenca S.* Cyber Threat Discovery from Dark Web // EPiC SeriesinComputing. 2019. № 64. P. 174–183.
10. *Rogers E. M., Singhal A., Quinlan M. M.* Diffusion of Innovations. New York: Free Press, 2002. DOI: https://doi.org/10.4324/9780203710753-35.
11. *Bass F. M.* A new product growth model for consumer durables // INFORMS. 1969. № 15 (5). P. 215–227. DOI: https://doi.org/10.1287/mnsc.15.5.215.
12. *Mansfield E.* Technical Change and the Rate of Imitation // Econometrica. 1961. № 29 (4). DOI: https://doi.org/10.2307/1911817.
13. *Hagerstrand T.* Innovation diffusion as a spatial process. Chicago: University of Chicago Press, 1967. DOI: https://doi.org/10.1111/j.1538-4632.1969.tb00626.x.
14. Свидетельство о государственной регистрации программы для ЭВМ 2019613098 Российская Федерация. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» / И. Н. Костюлин, А. В. Наумова, С. А. Овчинников, А. А. Пушкин, Ю. И. Худой; заявитель и правообладатель Закрытое акционерное общество «Перспективный мониторинг» (ЗАО «ПМ»). № 2019612022; заявл. 01.03.2019; опубл. 07.03.2019.
15. *Dargahi T., Dehghantanha A., Nikkhah Bahrami P., Conti M., Bianchi G., and Benedetto L.* A Cyber-Kill-Chain based taxonomy of crypto-ransomware features // Journal of Computer Virology and Hacking Techniques. 2019. P. 277–305.
16. The Cyber Kill Chain framework [Электронный ресурс]. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 29.12.2020).

Статья поступила в редакцию 20.11.2021.

Макарова Ольга Сергеевна

аспирант, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, e-mail: o.s.makarova@urfu.ru.

Поршнев Сергей Владимирович

д.т.н, профессор, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина (620075, Екатеринбург, пр. Ленина, 51), e-mail: sergey_porshnev@mail.ru.

Confirmation of the mathematical model adequacy describing the dynamics of implementing a computer attack possibility in time

O. Makarova, S. Porshnev

One of the urgent problems of information security at the moment is the lack of a unified approach for predicting computer attacks that is confirmed by both international and Russian experts as well as by practice. The paper proposes a mathematical model describing the dynamics of the computer attack in time built on the basis of the Diffusion of Innovations Theory. The substantiation of the possibility of using the Diffusion of Innovations Theory is given; the specifics of cybercrimes from other types of crimes are described. The adequacy of the proposed model is confirmed, in particular, by full-scale modeling of cyber-attacks on the organization's resources via the Internet site. The data of practical experiments confirm the mathematical model; in particular, the probability function of the cyber-attack implementation in time, i.e. the change in the number of infected nodes in time can be approximated using an s-shaped Pearl curve or a cascade model. The optimality of this approximation is proved by the method of least squares.

Keywords: computer attack, Pearl–Reed curves, theory of diffusion of innovations, dynamics of the spread of computer attack, full-scale modeling, computer attack on the resources of the organization via website, approximation.