МОДЕЛЬ КОМПЬЮТЕРНОЙ АТАКИ ТИПА «PHISHING» НА ЛОКАЛЬНУЮ КОМПЬЮТЕРНУЮ СЕТЬ

Добрышин М.М.[1], Закалкин П.В.[2]

Цель статьи: *доведение до специалистов в сфере информационной безопасности и научных сотрудников выявленных аналитических зависимостей, учитывающих параметры, характеризующие процесс ведения компьютерных атак типа «Phishing». Новые зависимости обеспечивают повышение достоверности результатов оценки защищенности локальной компьютерной сети, имеющей доступ к мировому информационному пространству от указанной угрозы.*

Метод исследования: *имитационное моделирование компьютерных атак типа «Phishing» и определение аналитической модели на основании аппроксимации результатов моделирования.*

Полученный результат: *создан инструментарий для инженерно-технического персонала позволяющий оценить защищенность локальной компьютерной сети от компьютерной атаки типа «Phishing» и при неудовлетворительном результате определить мероприятия по защите сети.*

Ключевые слова: *имитационная модель, аналитическая модель, моделирование, компьютерная атака типа «Phishing».*

DOI:10.21681/2311-3456-2021-2-17-25

Введение

Одним из основных негативных факторов, влияющих на состояние информационной безопасности Российской Федерации, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Постоянно повышается сложность, увеличиваются масштабы и растет скоординированность кибервоздействий на объекты критической инфраструктуры, усиливается разведывательная деятельность иностранных государств в отношении Российской Федерации, а также нарастают угрозы применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической, экономической и социальной стабильности Российской Федерации[3] [1].

К критически важным объектам инфраструктуры государства относят системы и средства, которые настолько жизненно важны для страны, что нарушение их работы или уничтожение оказывает необратимое негативное воздействие на национальную и экономическую безопасность, здравоохранение, правопорядок и т.д.

Примером критически важных объектов инфраструктуры являются организации топливно-энергетического комплекса, поддерживающие работу промышленных и оборонных производств, а также других стратегических объектов. Энергетика обеспечивает жизнедеятельность городов, больниц, телекоммуникационных станций, правительственных учреждений и других социально значимых объектов. Нарушение работы критически важных объектов инфраструктуры государства может привести к дестабилизации обстановки в отдельно взятом городе и стране в целом [2-3].

Отличительной чертой всей критической инфраструктуры на планете является ее функционирование посредством мирового киберпространства, что позволяет оказывать деструктивное воздействие на военные системы, объекты экономики и т.д. любого государства без непосредственного вторжения на территорию страны и объявления войны. Практически любым объектом критической инфраструктуры (без привязки к его географическим координатам) из любой точки планеты посредством киберпространства возможно осуществлять как управление, так и его перевод в режим функционирования соответствующий собственным интересам вплоть до полного отключения. При этом объекты воздействия не уничтожаются физически и их восстановление после достижения поставленных целей не вызывает затруднений для атакующей стороны. Крайним случаем является перевод объекта в критический режим функционирования приводящий к разрушению объекта [4-6].

Данный тип сложных атак преимущественно на инфраструктуру государственных и военных объектов, целых отраслей и конкретных компаний называют APT-атаками (Advanced Persistent Threat). Ежегодно количество APT-атак возрастает, по состоянию на 2019 г. доля проведенных APT-атак по отраслям выглядит сле-

1 Добрышин Михаил Михайлович, кандидат технических наук, сотрудник Академии ФСО России, г. Орел, Россия. E -mail: Dobrithin@ya.ru

2 Закалкин Павел Владимирович, кандидат технических наук, докторант, Военная академия связи, г. Санкт Петербург, Россия. E -mail: pzakalkin@mail.ru

3 1) Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ 05.12.2016 г. № 646.
2) Военная доктрина Российской Федерации. Утверждена Президентом РФ 25.12.2014 г. № ПР-2976.

дующим образом: государственные учреждения (70%), промышленные компании (60%), финансовая отрасль (45%), топливно-энергетический комплекс (41%)[4].

Злоумышленники совершенствуют и разрабатывают новые подходы, направленные на хищение защищаемой информации (персональные данные, реквизиты банковских карт, конфиденциальная корпоративная информация) из локальных сетей компаний. В настоящее время существуют организационные и организационно-технические подходы, позволяющие физически разграничить доступ к защищаемой информации в локальных компьютерных сетях, однако тенденции развития бизнеса требуют от должностных лиц оперативной обработки данных и принятию решений, что приводит к противоречию между требованиями к защите информации и ведению бизнеса [7-8].

Для устранения указанного противоречия в настоящее время применяют различные технические решения [9-11], которые должны обеспечить требуемый уровень защищенности, однако статистические данные, а также «резонансные» инциденты информационной безопасности, освещаемые в средствах массовой информации свидетельствуют об их недостаточной эффективности. Данный недостаток обусловлен тем, что доля целенаправленных атак занимает существенную часть от всей совокупности проводимых атак.

Наиболее часто и успешно используемой техникой в рамках APT-атак является «Phishing» – одна из техник социальной инженерии, основной целью которой является получение доступа к конфиденциальным данным пользователей. Согласно отчета Positive Technologies порядка семи из девяти группировок проникают в инфраструктуру посредством «Phishing», далее по популярности идет компрометация ресурсов сторонних организаций (с последующим проникновением в целевую систем) и компрометация сайтов, посещаемых сотрудниками целевой организации (проникновение в целевую систему посредством посещения пользователе зараженного сайта).

Организация защиты от атаки типа «Phishing» требует применение комплекса мероприятий, как на техническом, так и на организационно-техническом уровне, однако применяемый научно-методический аппарат [12-15] описывает процессы выявления атак типа «Phishing» исключительно на техническом уровне, что приводит к тому, что существенная часть атак становятся успешными.

Для устранения указанного недостатка и повышения защищенности локальных компьютерных сетей от атак типа «Phishing» необходимо разработать модель позволяющую выявлять уязвимости на организационно-техническом уровне, для их дальнейшего устранения.

4 1) Positive Research 2018 Сборник исследований по практической безопасности 2018 // Positive Technologies. С. 206.
2) Positive Research 2019 Сборник исследований по практической безопасности 2019 // Positive Technologies. С. 297.
3) Positive Research 2020 Сборник исследований по практической безопасности 2020 // Positive Technologies. С. 274.

Постановка задачи

Задача моделирования заключается в повышении достоверности результатов моделирования сетевой атаки типа «Phishing» за счет учета количественного и качественного состава отправляемых электронных сообщений содержащих вредоносный код, состава защищаемой локальной компьютерной сети и возможностей систем обнаружения и противодействия компьютерным атакам и антивирусного программного обеспечения блокировать электронные сообщения содержащих вредоносный код.

Целью моделирования является выявление зависимости вероятности успешной компьютерной атаки типа «Phishing» на локальную компьютерную сеть от времени, учитывающую вероятность пропуска системой обнаружения предупреждения о компьютерных атаках (СОПКА) сообщения содержащего вредоносное («зараженного») программное обеспечения (ПО); вероятность прочтения «зараженного» сообщения пользователем персонального компьютера входящего в локальную сеть (ПК) на которое отправлено сообщение и вероятность успешной активации вредоносного кода (перехода по ссылке на «фишинговый» ресурс).

Основными исходными данными являются количество персональных компьютеров в защищаемой локальной сети ($N_{ПК}$,$N_{ПК}=1,2,...,n$) обладающих ($N_{адр}$,$N_{ПК} \in N_{адр}$) IP-адресом; количество пользователей в защищаемой локальной сети (m); количество сигнатур в СОПКА ($N_{СИГ}$,$N_{СИГ}=1,2,...,s$); периодичность обновления антивирусных баз j-го персонального компьютера ($t^{i}_{ОБН}j=0,1,2,...,n$); максимальное допустимое в защищаемой сети время между обновлениями антивирусных баз ($t^{max}_{обн}$); количество персональных компьютеров в атакующей сети (z); количество электронных сообщений с вредоносным кодом применяемых при однократной рассылке электронных сообщений с вредоносным кодом ($N_{сообщ}$); количество типов уникальных по содержанию электронных сообщений с вредоносным кодом при однократной рассылке вредоносных сообщений ($N^{уник}_{сообщ}$); количество повторений рассылок электронных сообщений с вредоносным кодом (V); порядковый номер рассылки электронных сообщений ($i=0,1,2, ... , V$) в заданный период времени; количество серверов получателей защищаемой информации ($N_{серв}$).

Основные допущения и ограничения: рассматриваются компьютеры, имеющие доступ к мировому информационному пространству; временной ресурс сил и средств ограничен; средние значения параметров атак соизмеримы со среднестатистическими значениями; в локальной сети используется единая СОА с ограниченным ресурсом.

Структура и содержание имитационной модели компьютерной атаки типа «Phishing» на локальную компьютерную сеть

Процесс моделирования компьютерной атаки типа «Phishing» на локальную сеть заключается в поэтапной имитации: обнаружения и блокирования системой обнаружения и противодействия компью-

терным атакам электронных сообщений содержащих вредоносный код; обнаружения и блокирования антивирусным программным обеспечением электронных сообщений содержащих вредоносный код, прочтения электронного сообщения пользователями персональных компьютеров, а также обнаружения и блокирования системой обнаружения и противодействия компьютерным атакам процесса передачи сообщений на серверы злоумышленников. Последовательность функционирования модели представлен на рисунке 1.

В блоке 1 на основании анализа значений параметров рассматриваемой локальной сети и статистических значений сетевых атак типа «fishing» вводят исходные данные.

В блоке 2 формируют модель защищаемой локальной сети связи получающей доступ к ресурсам ЕСЭ (рис. 2). Модель состоит из n персональных компьютеров (ПК-1, ПК-2, ..., ПК-n) (каждый персональный компьютер обладает уникальным IP-адресом) имитирующих защищаемые компьютеры локальной сети; на каждый персональный компьютер устанавливается антивирусное программное обеспечение; средств обнаружения и противодействия компьютерных атак (Э-1); маршрутизатора (М-1) обеспечивающего соединение компьютеров защищаемой локальной сети между собой; маршрутизатора (М-2) обеспечивающего соединения локальной сети с единой сетью электросвязи, а также маршрутизатора (М-3) имитирующего маршрутизатора провайдера обеспечивающего соединение с сервисами единой сети электросвязи; почтовый сервер и средство обнаружения и противодействия компьютерным атакам (Э-2), через который защищаемая локальная сеть получает электронные письма.

В блоке 3 настраивают средства обнаружения и противодействия компьютерным атакам (Э-1, Э-2) (задают количество сигнатур обеспечивающих обнаружение атак; определяют перечень IP-адресов с которыми запрещено взаимодействие).

В блоке 4 формируют модель компьютерной сети (Botnet) имитирующей сеть, которая осуществляет рассылку электронных сообщений с вредоносным кодом. Модель состоит из группы персональных компьютеров (Bot-1, Bot-2, ..., Bot-z) соединенных между собой маршрутизатором (М-4), группы персональных компьютеров (ПК-С1, ПК-С2,..., ПК-Cs) имитирующих серверы на которые отправляются сообщения после заражения вредоносным кодом персональных компьютеров защищаемой локальной сети.

В блоке 5 формируют перечень типов электронных писем с вредоносным кодом. Каждый тип электронного письма обладает уникальным IP-адресом отправки; атрибутами различных сетевых сервисов и служб (служба рассылки сообщений провайдеров услуг связи, банков), государственных министерств или ведомств, интернет ресурсов (магазины, рекламные агентства); различным вредоносным кодом (язык программирования, типовые блоки, способы активации).

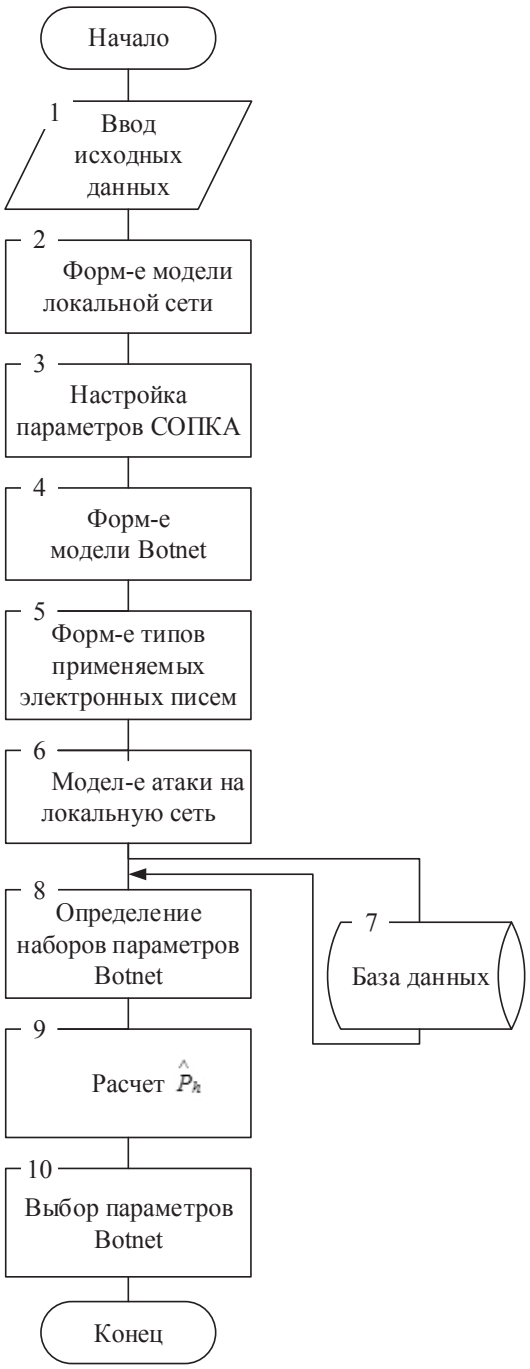

Рис. 1. Последовательность функционирования модели компьютерной атаки типа «Phishing» на локальную сеть

В блоке 6.1 Botnet отправляет на IP-адреса персональных компьютеров защищаемой сети электронные сообщения с вредоносным кодом. При моделировании изменяют количество электронных сообщений с вредоносным кодом $(1,2,...,N_{\text{сообщ}})$ отправляемых на один персональный компьютер; количество типов уникальных по содержанию электронных сообщений с вредоносным кодом $(1,2,...,N^{\text{уник}}_{\text{сообщ}})$ и количество сигнатур в СОПКА (Э-1, Э-2) $(N_{\text{СИГ}}, N_{\text{СИГ}}=1,2,...,s)$.

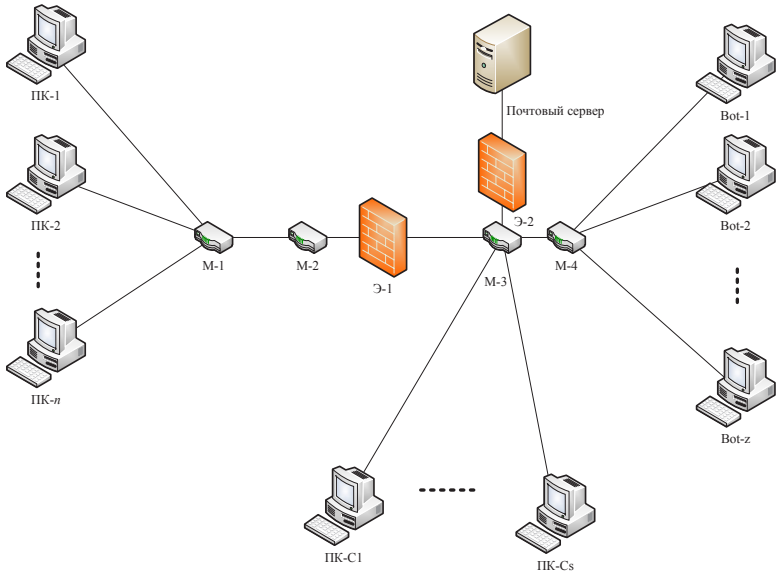

Рис. 2. Функциональная схема проведения компьютерной атаки типа «Phishing» на локальную сеть

В блоке 6 моделируют атаку на локальную сеть (рис. 3).

В блоке 6.2 на основании статистических данных полученных при сравнении количества отправленных электронных сообщений из Botnet и обнаруженных сообщений СОПКА (Э-1, Э-2) определяют типы электронных сообщений ($N^{\text{уник}^*}_{\text{сообщ}}$), которые СОПКА неспособна обнаружить. Определяют количество электронных сообщений прошедших в защищаемую локальную сеть. Полученные значения сохраняют в базу данных (блок 7).

В блоке 6.3 имитируют обработку электронных сообщений с вредоносным кодом на персональном компьютере. При имитации обработки электронных сообщений изменяют типы электронных сообщений ($N^{\text{уник}^*}_{\text{сообщ}}$), которые СОПКА неспособна обнаружить, количество повторений рассылок электронных сообщений с вредоносным кодом $(1,2,\ldots,V)$ в заданный период времени, а также осуществляют обновление антивирусных баз $(t^{j}_{\text{обн}} = t^{j\,min}_{\text{обн}}, \ldots, t^{max}_{\text{обн}})$.

В блоке 6.4 на основании анализа количества поступивших электронных сообщений с вредоносным кодом на персональный компьютер и обнаруженных антивирусным программным обеспечением определяют количество не обнаруженных электронных писем ($N^{\text{уник}^*}_{\text{сообщ}}$), количество повторений рассылок электронных сообщений $(1,2,\ldots,V)$ и время между обновлениями антивирусных баз $((t^{*}_{\text{обн}}))$ при котором антивирусное программное обеспечение не способно обнаружить электронные сообщения с вредоносным кодом. Полученные значения сохраняют в базу данных (блок 7).

В блоке 6.5 имитируют прочтение пользователем (m) защищаемой локальной сети электронных сообщений с вредоносным кодом ($N^{\text{уник}^*}_{\text{сообщ}}$), необнаруженных антивирусным программным обеспечением. Процесс имитации основан на розыгрыше вероятностей прочтения. Опорные вероятности формируют на основании соотношения социального профиля пользователя и атрибутов электронного сообщения.

В блоке 6.6 определяют количество персональных компьютеров, на которых активирован вредоносный код из полученных электронных писем. Полученные значения сохраняют в базу данных (блок 7).

В блоке 6.7 отправляют с зараженного вредоносным кодом персонального компьютера на серверы получатели защищаемой информации ($N_{\text{серв}}$) электронные сообщения; работу антивирусного программного обеспечения и СОПКА. При имитации отправки сообщений на сервер получателей защищаемой информации на каждом зараженном персональном компьютере изменяют: IP-адреса сервера получателя защищаемой информации; сетевые протоколы, с помощью которых отправляют сообщения; количество сигнатур в антивирусном программном обеспечении и СОПКА.

В блоке 6.8 на основании статистических данных определяют количество серверов получателей защищаемой информации ($N^{*}_{\text{серв}}$), а также сетевые протоколы, с помощью которых отправляют сообщения; количество сигнатур антивирусного программного обеспечения и СОПКА при которых данные сообщения были переданы. Полученные значения сохраняют в базу данных (блок 7).

В блоке 8 на основании полученных из блока 7 данных объединяют значения параметров Botnet в h наборов.

В блоке 9 рассчитывают значение статистической вероятности успешной атаки ($\hat{P}_h$) для h-го набора значений параметров Botnet:

$$\hat{P}_h = \frac{N^{\text{зар}}_h}{N^{\text{пз}}_h}.$$

где $N_h^{зар}$ – количество успешно зараженных персональных компьютеров при h– наборе, $N_h^{пз}$– количество атакуемых компьютеров.

Рассчитанные значения сохраняют в базе данных (блок 7).

В блоке 10 на основании анализа значений вероятности успешной атаки ($\hat{P}_h$) определяют h-й набор значений параметров Botnet, при котором вероятность заражения персонального компьютера достигает максимального значения. При одинаковых значениях вероятности успешной атаки ($\hat{P}_h$) выбор h-го набора значений параметров Botnet производит оператор.

Рис. 3. Последовательность функционирования блока моделирования компьютерной атаки типа «Phishing» на локальную сеть

Моделирование компьютерной атаки типа «Phishing» на локальную компьютерную сеть

Представленная модель реализована в имитационной среде AnyLogic.

Исходные данные, используемые при моделировании, представлены в таблице 1. Исходные данные, не изменяемые при моделировании: $N_{сообщ}$=100, N_{IP}=70, n =70 $t_{обн}^{max} = 1440$. Результаты моделирования представлены на рисунках 4-6.

Обработка результатов моделирования, определение аналитической модели компьютерной атаки типа «Phishing» на локальную компьютерную сеть

На основании аппроксимации результатов имитационного моделирования (аппроксимация проводилось при помощи MatLab R 2012a, программы для ЭВМ Advanced Grapher ver. 2.2) получены следующие зависимости:

Вероятность успешной компьютерной атаки типа «Phishing» на локальную сеть:

$$P^{phishing}(t)=P_1(t)\cdot P_2(t)\cdot P_3(t) \quad (1)$$

где $P_1(t)$ – вероятность пропуска СОПКА сообщения содержащего вредоносное («зараженного») ПО; $P_2(t)$ – вероятность прочтения «зараженного» сообщения пользователем ПК на которое отправлено сообщение; $P_3(t)$ – вероятность успешной активации вредоносного кода (перехода по ссылке на фишинговый ресурс).

$$P_1 = K_1^{\frac{N_{сообщ}(i-1)}{N_{сообщ}^{уник}100}}, \quad (2)$$

где K_1^i – коэффициент полноты используемых электронных адресов локальной сети при проведении атаки; $N_{сообщ}$ – количество электронных сообщений в одной «волне» рассылки; $N_{сообщ}^{уник}$ – количество уникальных по содержанию электронных сообщений в одной «волне» рассылки; i – порядковый номер «волны» рассылки электронных сообщений $(1,2,\dots,V$, V – количество «волн» рассылки электронных сообщений в течение атаки);

$$K_1 = \frac{N_{IP\,n}^{атак\,i}}{N_{IP}}, \quad (3)$$

$N_{IP\,n}^{атак\,i}$ – количество атакуемых IP адресов при i –ой «волне» рассылки; N_{IP} – количество IP адресов в локальной сети ОГВ $(N_{IP\,n}^{атак\,i} \in N_{адр};\ n = 0,1,2,\dots,N_{адр},\ i = 0,1,2\dots V)$;

$$P_2^i = 1 - (K_2)^i, \quad (4)$$

где K_2 – количество пользователей на одной ПК в защищаемой локальной сети:

$$K_2 = \frac{n}{m}, \quad (5)$$

где n – количество ПК в защищаемой локальной сети; m – количество пользователей в защищаемой локальной сети;

$$P_3^i = (K_2)^{\frac{i-1}{4}}, \quad (6)$$

Таблица 1

Исходные данные, применяемые при моделировании

Параметр	$N_{\text{сообщ}}^{\text{уник}}$	$N_{IP\,n}^{\text{атак}\,i}$	i	m	$t_{\text{обн}}^{j}$
Диапазон изменения	1–100	1–70	1–10	1–3	1–1440
Шаг изменения	1	1	1	1	60

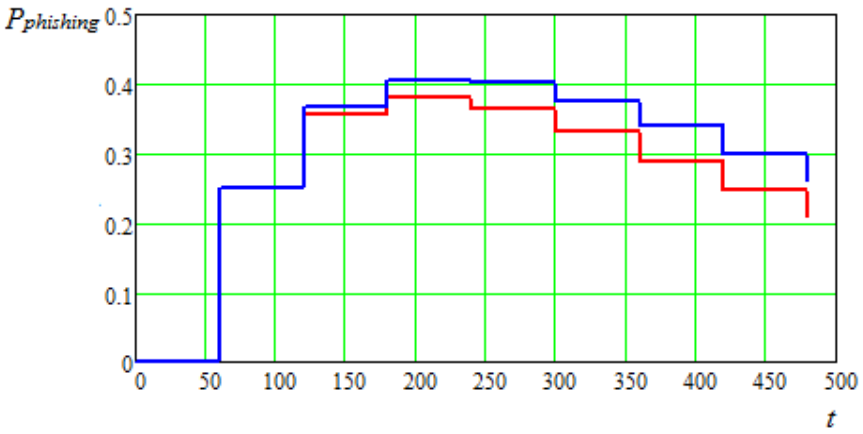

Рис. 4. Зависимость вероятности успешной КА типа «Phishing» от времени при различном количестве уникальных сообщений в одной «волне» рассылке сообщений

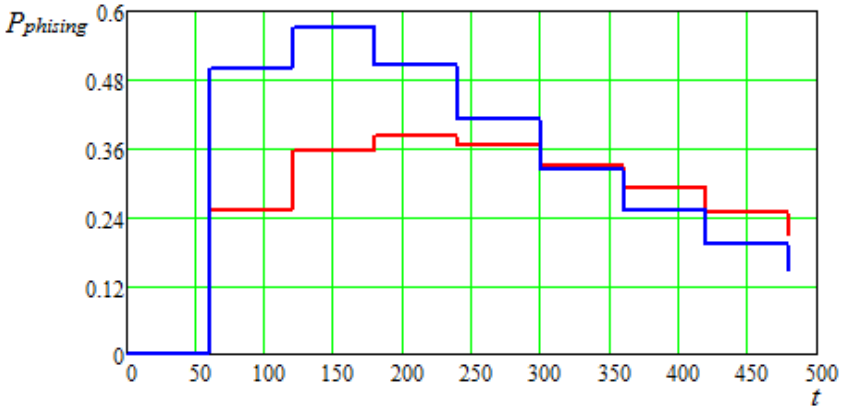

Рис. 5. Зависимость вероятности успешной КА типа «Phishing» от времени при различном количестве IP-адресов, на которые осуществляется рассылка сообщений

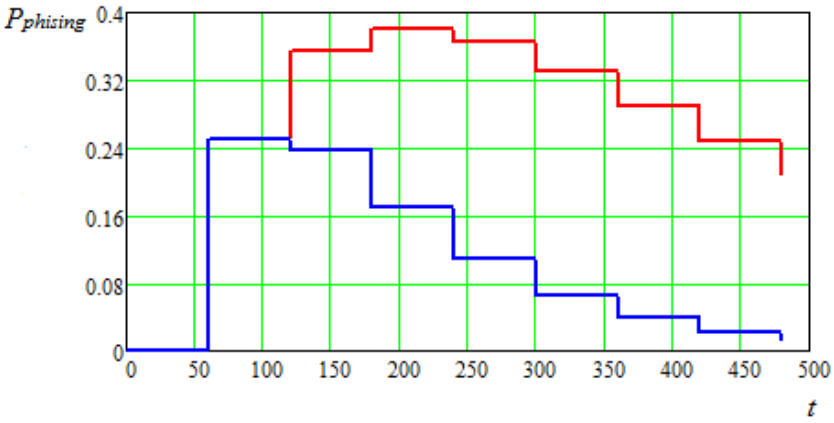

Рис. 6. Зависимость вероятности успешной КА типа «Phishing» от времени при различном времени обновления антивирусных баз СОПКА

где $K_з$ – относительная актуальность баз средств СОПКА в защищаемой локальной сети:

$$K_3(t) = \frac{\sum_{j=1}^{n} t_{\text{обн}}^{j}}{n \cdot t_{\text{обн}}^{max}}, \qquad (7)$$

где $t_{\text{обн}}^{j}$ – периодичность обновления антивирусных баз на j-й ПК ($j=0,1,2\ldots n$); $t_{\text{обн}}^{max}$ – максимально допустимое в защищаемой сети время между обновлениями антивирусных баз.

Выводы

Использование разработанного предложения позволяет на основе аппроксимации результатов имитационного моделирования получить аналитическую зависимость вероятности успешной компьютерной атаки типа «Phishing» на локальную сеть. Новая аналитическая модель позволяет оценить защищенность локальной компьютерной сети, а также эффективность разработанных мероприятий защиты от компьютерной атаки типа «Phishing».

Оценка эффективности предлагаемого предложения проводилась на основании сравнения достоверности результатов моделирования компьютерной атаки типа «Phishing» с одним из известных решений. Результаты расчета показывают повышение достоверности результатов моделирования на 21,7 %. Таким образом, поставленная задача исследования выполнена.

Научная новизна разработанной модели заключается в том, что она позволяет за счет учета новых параметров, характеризующих процесс проведения компьютерной атаки типа «Phishing» в отношении локальной компьютерной сети, получить временное представление и новые вероятностные зависимости. Элементы разработанной модели частично реализованы в программе для ЭВМ [16].

Литература

1. Добрышин М.М. Модель разнородных компьютерных атак проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. № 12. С. 31-35.
2. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16-21.
3. Стародубцев Ю.И., Бухарин В.В., Семенов С.С. Техносферная война // Военная Мысль. 2012. № 7. С. 22-31.
4. Дылевский И.Н., Базылев С.И., Запивахин О.В., Комов С.А. и др. О взглядах администрации США на киберпространство как новую сферу ведения военных действий // Военная мысль. 2020. № 10. С.22-29.
5. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1(29). С. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9
6. Дурнев Р.А., К.Ю. Крюков, Дедученко Ф.М. Предупреждение техногенных катастроф, провоцируемых в ходе военных действий // Военная мысль. 2019. № 10. С. 41-48.
7. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2 (30). С. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49
8. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23

9. Бегаев А.Н., Добрышин М.М., Закалкин П.В., Реформат А.Н., Рауткин Ю.В. Комплексный алгоритм мониторинга защищенности узлов VPN от компьютерной разведки и DDOS-атак // Электросвязь. 2018. № 7. С. 46-52.
10. Гречишников Е.В., Добрышин М.М., Закалкин П.В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12. DOI:10.21681/2311-3456-2016-3-4-12.
11. Бегаев А.Н., Гречишников Е.В., Добрышин М.М., Закалкин П.В. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий // Вопросы кибербезопасности 2018. № 3 (27). С. 2-8. DOI: 10.21681/2311-3456-2018-3-02-08.
12. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. СПб.: Изд-во «Наукоемкие технологии», 2017. 120 с.
13. Паршуткин А.В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.
14. Анисимов В.В., Бегаев А.Н., Стародубцев Ю.И. Модель функционирования сети связи с неизвестным уровнем доверия и оценки её возможностей по предоставлению услуги VPN с заданным качеством // Вопросы кибербезопасности. 2017. № 1 (19). С. 6-15. DOI: 10.21681/2311-3456-2017-1-6-15.
15. Еремеев М.А., Аллакин В.В., Будко Н.П. Модель наступления критического события информационной безопасности в информационно-коммуникационной системе // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 6. С. 52-60.5
16. Свидетельство о государственной регистрации программы для ЭВМ № 2019610015. Программа расчета вероятности осуществления злоумышленником сетевой атаки типа «Фишинг». / М. М. Добрышин, П.В. Закалкин, Р.В. Гуцын. – опубл. 10.01.2019 г. Бюл. № 1

MODEL OF A “PHISHING” TYPE OF COMPUTER ATTACK ON A LOCAL COMPUTER NETWORK

Dobryshin M. M.[5], Zakalkin P. V.[6]

Abstract: *The purpose of the article is to inform information security specialists and researchers of the identified analytical dependencies that take into account the parameters that characterize the process of conducting computer attacks of the “Phishing” type. New dependencies provide an increase in the reliability of the results of assessing the security of a local computer network that has access to the global information space from the specified threat.*

Research method: *simulation of computer attacks of the “Phishing” type and determination of the analytical model based on the approximation of the simulation results.*

The result: *a set of tools for engineering and technical personnel has been created to assess the security of a local computer network from a “Phishing” type of computer attack and, if the result is unsatisfactory, determine measures to protect the network.*

Keywords: *simulation model, analytical model, simulation, computer attack of the “Phishing” type.*

References

1. Dobryshin M.M. Model’ raznorodnyh komp’juternyh atak provodimyh odnovremenno na uzel komp’juternoj seti svjazi // Telekommunikacii [Telecommunications] 2019. No 12. pp. 31-35.
2. Starodubcev Ju.I., Zakalkin P.V., Ivanov S.A. Tehnosfernaja vojna kak osnovnoj sposob razreshenija konfliktov v uslovijah globalizacii // Voennaja mysl’ [Military throught]. 2020. No 10. pp.16-21.
3. Starodubcev Ju.I., Buharin V.V., Semenov S.S. Tehnosfernaja vojna // Voennaja Mysl’ [Military throught] 2012. No 7. pp. 22-31.
4. Dylevskij I.N., Bazylev S.I., Zapivahin O.V., Komov S.A. i dr. O vzgljadah administracii SShA na kiberprostranstvo kak novuju sferu vedenija voennyh dejstvij // Voennaja mysl’ [Military throught] 2020. No 10. pp.22-29.
5. Romashkina N.P. Global’nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. No 1(29). pp. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9.
6. Durnev R.A., K.Ju. Krjukov, Deduchenko F.M. Preduprezhdenie tehnogennyh katastrof, provociruemyh v hode voennyh dejstvij // Voennaja mysl’ [Military throught] 2019. No 10. pp. 41-48.
7. Gas’kova D.A., Massel’ A.G. Tehnologija analiza kiberugroz i ocenka riskov narushenija kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. No 2 (30). pp. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49.

5 Mikhail Dobryshin, Ph.D., Fellow of the Academy and FSO of Russia, Orel, Russia. E-mail: Dobrithin@ya.ru
6 Pavel Zakalkin, Ph.D., Military Academy of Communications, St. Petersburg, Russia. E-mail: pzakalkin@mail.ru

8. Karchija A.A., Makarenko G.I., Seregin M.Ju. Sovremennye trendy kiberugroz i transformacija ponjatija kiberbezopasnosti v uslovijah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. 2019. No 3 (31). pp. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23.
9. Begaev A.N., Dobryshin M.M., Zakalkin P.V., Reformat A.N., Rautkin Ju.V. Kompleksnyj algoritm monitoringa zashhishhennosti uzlov VPN ot komp'juternoj razvedki i DDOS-atak // Jelektrosvjaz' [Telecommunication]. 2018. No 7. pp. 46-52.
10. 10. Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Model' uzla dostupa VPN kak ob'ekta setevoj i potokovoj komp'juternyh razvedok i DDoS-atak // Voprosy kiberbezopasnosti. 2016. No 3 (16). pp. 4-12. DOI:10.21681/2311-3456-2016-3-4-12.
11. Begaev A.N., Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. Predlozhenie po ocenke sposobnosti uzla komp'juternoj seti funkcionirovat' v uslovijah informacionno-tehnicheskih vozdejstvij // Voprosy kiberbezopasnosti. 2018. No 3 (27). pp. 2-8. DOI: 10.21681/2311-3456-2018-3-02-08.
12. Drobotun E.B. Teoreticheskie osnovy postroenija sistem zashhity ot komp'juternyh atak dlja avtomatizirovannyh sistem upravlenija. SPb.: «Naukoemkie tehnologii», 2017. 120 p.
13. Parshutkin A.V. Konceptual'naja model' vzaimodejstvija konfliktujushhih informacionnyh i telekommunikacionnyh sistem // Voprosy kiberbezopasnosti. 2014. No 5 (8). pp. 2-6.
14. Anisimov V.V., Begaev A.N., Starodubcev Ju.I. Model' funkcionirovanija seti svjazi s neizvestnym urovnem doverija i ocenki ejo vozmozhnostej po predostavleniju uslugi VPN s zadannym kachestvom // Voprosy kiberbezopasnosti. 2017. No 1 (19). pp. 6-15. DOI: 10.21681/2311-3456-2017-1-6-15.
15. Eremeev M.A., Allakin V.V., Budko N.P. Model' nastuplenija kriticheskogo sobytija informacionnoj bezopasnosti v informacionno-kommunikacionnoj sisteme // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli [Science-Intensive technologies in space research of the Earth]. 2017. Vol. 9. No 6. pp. 52-60.
16. Svidetel'stvo o gosudarstvennoj registracii programmy dlja JeVM № 2019610015. Programma rascheta verojatnosti osushhestvlenija zloumyshlennikom setevoj ataki tipa «Fishing». Dobryshin M. M., Zakalkin P.V., Gucyn R.V.. – opubl. 10.01.2019 g. Bjul. No 1.