

уменьшает время реализации данных алгоритмов для бинарных изображений. Для операций замыкания и размыкания исключена повторная замена точек форм, которая бы осуществлялась при по-

очередном использовании модифицированных операций эрозии и наращивания.

*Работа выполнена при поддержке РФФИ, проект № 06-8-00751.*

#### СПИСОК ЛИТЕРАТУРЫ

1. Маргос П., Серра Дж. Морфологические системы для обработки многомерных сигналов // Труды института инженеров по электротехнике и радиоэлектронике. — 1990. — Т. 78. — № 4. — С. 109–132.
2. Пытьев Ю.П. Морфологический анализ изображений // Доклады АН СССР. — 1983. — Т. 269. — № 5. — С. 1061–1064.
3. Пытьев Ю.П. Задачи морфологического анализа изображений // Математические методы исследования природных ресурсов Земли из космоса / Под ред. В.Г. Золотухина. — М.: Наука, 1984. — С. 41–83.
4. Абламейко С.В., Лагуновский Д.М. Обработка изображений. — Минск: Амафрей, 2000. — 304 с.
5. Chen. T. A pseudo top-hat mathematical morphological approach to edge detection in dark regions // Pattern Recognition. — 2002. — V. 35. — № 1. — P. 199–210.
6. Sossa-Azuela J.H. Computing geometric moments using morphological erosions // Pattern Recognition. — 2001. — V. 34. — № 2. — P. 271–276.
7. Laganieri R. A morphological operator for corner detection // Pattern Recognition. — 1998. — V. 31. — № 11. — P. 1643–1652.
8. Pring Z. Document filters using morphological and geometrical features of characters // Image and Vision Computing. — 2001. — V. 19. — № 12. — P. 847–855.

УДК 004.056

## ФОРМАЛИЗАЦИЯ МОДЕЛИ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ КОДОВ

И.В. Давыдов, А.А. Шелупанов

Томский государственный университет систем управления и радиоэлектроники

E-mail: davidoffi@mail.ru, saa@keva.tusur.ru

*Рассмотрена модель совершения киберпреступлений, совершаемых с использованием вредоносных кодов. Проведена формализация предложенной модели, а также возможные меры противодействия на этапах совершения киберпреступления. Выделены аспекты исследования информационных следов этих преступлений на этапах расследования.*

Настоящее время — эпоха информационного общества, в котором компьютерные и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства — от решения проблем национальной безопасности, здравоохранения и управления транспортом до простого межличностного общения. Не секрет, что все эти системы хранят в себе информацию, которая порой бесценна. Не секрет и то, что в мире обязательно найдутся люди, которых эта информация так или иначе компрометирует, и они готовы пойти на многое, чтобы получить эту информацию или уничтожить ее.

Добиться поставленных целей возможно, если только пойти по двум сценариям: агентурным методом либо получить несанкционированный доступ к охраняемой информации программными средствами и осуществить задуманное. В случае агентурного метода эта процедура наверняка привлечет к себе внимание правоохранительных органов и спецслужб. В случае получения несанкционированного доступа программными средствами это будет практически незаметно, и, что особенно важно, на реализацию этого способа не потребуются значительные денежные вложения. Именно по

этим причинам получение несанкционированного доступа к охраняемой информации программными средствами в мире особо популярно [1, 2].

В большинстве случаев получение несанкционированного доступа достигается при помощи вредоносных кодов, реализованных на несовершенстве систем защиты программного обеспечения. В этом случае цели достигаются не при помощи общеизвестных и детектируемых вредоносных кодов, именуемых в хакерской среде как «Public», а при помощи специализированных и настроенных под строго определенные условия, не детектируемых ни одним антивирусным пакетом, вредоносных кодов, именуемых в хакерской среде как «Private». Стоимость таких «приватных» кодов исчисляется от 0,1 до нескольких сотен млн р. [3].

Особенностью киберпреступлений этого типа является то, что они совершаются по одной модели, содержащей четко выделяемые стадии: рекогносцировка (поверхностное изучение), сканирование (подробное изучение), составление карты (полное изучение), получение доступа к системе, расширение полномочий, «зомбирование» системы, кража информации и уничтожение следов. Схематично данная модель представлена на рис. 1.

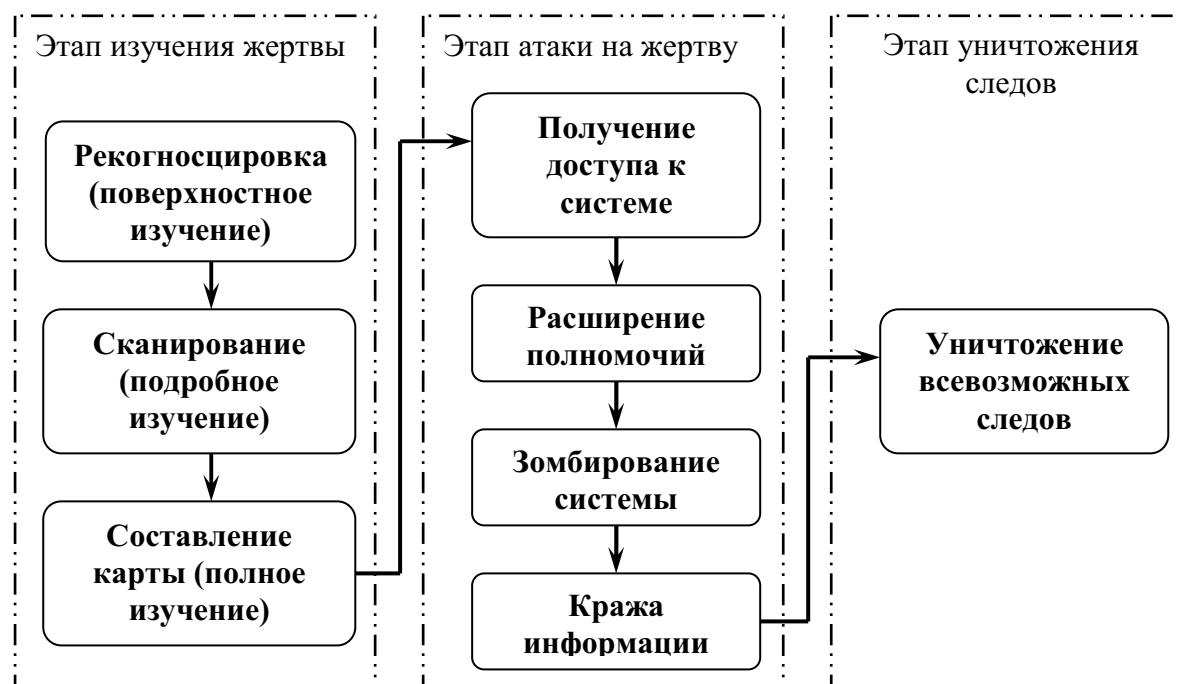


Рис. 1. Модель совершения киберпреступлений, совершаемых с использованием вредоносных кодов

«Зомбирование» системы достигается при помощи специализированного вредоносного кода, предназначенного для удаленного управления системой и основанное на организации и использовании несанкционированного доступа к системе.

Также необходимо отметить, что на стадии «зомбирования», атакованная система, управляемая злоумышленником, сама участвует в атаке на другие системы. Тем самым решается проблема нехватки вычислительных ресурсов и пропускной возможности канала атакующих по отношению к атакуемым системам. Именно поэтому периодические в глобальной сети проявляются информационные противоборства, естественно, незаконные и основанные на вышеописанном обстоятельстве.

Учитывая сказанное, можно оценить эффективность (*eff*) данного вида киберпреступлений, как оружия информационных противоборств [4]:

$$eff = \frac{n \cdot s}{t \cdot cost},$$

где  $n$  — число систем, которые могут быть поражены;  $s$  — число компьютеров, которые могут одновременно управляться серверной частью вредоносного кода, будучи не детектируемыми;  $t$  — время нахождения системы в состоянии «зомбирования»;  $cost$  — стоимость вредоносного кода, а также накладные расходы, связанные с их применением.

Проведенной оценкой нами установлено, что при использовании «базового» приватного кода

стоимостью около 10 тыс. р., со средним временем устойчивого зомбирования в 10 дн.<sup>1</sup>, с числом систем равным 20 и с тысячей компьютеров, одновременно управляемых серверной частью, численное значение эффективности будет равно 0,1. На первый взгляд эта цифра может показаться крайне малой, но необходимо отметить, что расчет проводится относительно затраченного рубля, а стоимость информации порой исчисляется десятками миллионов, поэтому реальное значение эффективности колоссально. Именно благодаря высокой эффективности, данный вид киберпреступлений с каждым годом становится все популярнее, и потому необходим научный подход в решении этой проблемы [6, 7].

Поскольку киберпреступления с использованием вредоносных кодов имеют собственные и отличные объект и субъект, специфический круг целей, определенную модель, специфический ущерб, уникальный алгоритм оперативных действий и расследования, данный вид преступлений подлежит формализации.

Для начала можно определить основные параметры модели совершения киберпреступления при помощи теоретико-множественного подхода.

В этом случае **злоумышленник** ( $X_1$ ) будет обладать следующими параметрами:

- доступные ему средства и методы;
- применяемые им средства и методы;

<sup>1</sup> Стоит отметить, что по данным компании Symantec среднее время, в котором система устойчиво находится в состоянии «зомбирования», обусловлено частотой актуализации общедоступных антивирусных баз, отказом в обслуживании аппаратной части системы и полной сменой программной части системы [5].

- профессиональное образование;
- правовая образованность в части совершаемого деяния;
- возраст;
- социальный статус в сети;
- принадлежность к организованным преступным группировкам.

**Объект ( $Y_n$ )**, на который происходит посягательство, будет обладать следующими параметрами:

- стоимость ресурса;
- величина уязвимости;
- частота актуализации;
- объем хранимой информации;
- степень категорирования информации;
- ответственные за объект лица;
- широта использования хранимой информации;
- фактологическая или документальная информация размещена на ресурсе;
- максимально возможная величина ущерба при несанкционированном доступе;
- возможно вменяемые статьи УК РФ при атаке злоумышленника;
- глубина защищенности;
- несанкционированное удаленное управление.

**Ущерб ( $D_n$ )**, наносимый объекту злоумышленником, будет состоять из следующих параметров:

- материальный;
- физический;
- иной.

**Внешнее воздействие ( $W_n$ )**, влияющее на работу объекта, будет состоять из таких параметров как:

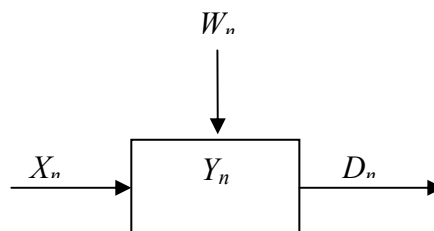
- погодные условия;
- аварии, сбои;
- халатность обслуживающего систему персонала;
- ошибки, допущенные при разработке системы.

Таким образом, совершаемое киберпреступление ( $CC_n$ ) будет представлено в виде множества, состоящего из подмножеств характеризующих объект, субъект, ущерб и внешнее воздействие:  $CC_n = \{X_n, Y_n, D_n, W_n\}$ .

Модель киберпреступления будет выглядеть как модель «черного ящика», на который поступают определенные воздействия и вследствие внутреннего взаимодействия получается некий ответ. Схематично данная модель представлена на рис. 2.

Представляют интерес для подробного рассмотрения параметры объекта на этапе зомбирования

системы, поскольку в данном состоянии система «двулична» — она и жертва, и атакующий, она и защищена, и беззащитна. Отклонение отдельных параметров на стадии зомбирования от нормального<sup>2</sup> состояния можно представить в виде таблицы.



**Рис. 2.** Модель совершения киберпреступлений на примере «черного ящика»

**Таблица.** Отклонение отдельных параметров на стадии зомбирования от нормального состояния. Значения приведены лишь для сравнения порядка величин

Параметр объекта	Значение в состоянии	
	Нормальном	Зомбирования
Уровень уязвимости	30 из 100	80 из 100
Объем хранимой информации, Мб	200	201
Максимально возможная величина ущерба при несанкционированном доступе, млн р.	1,0	1,1
Глубина защищенности, уровень	пользователей	root (системы)
Несанкционированное удаленное управление	отсутствует	имеется

Оценки уровня уязвимости, приведенные по данным фирмы Internet Security Systems, означают, что в состоянии зомбирования уровень уязвимости системы выше из-за возможности переподчинения «зомби-сети»<sup>3</sup>, когда у злоумышленника был перехвачен пароль на доступ к несанкционированному удаленному управлению. По этой же причине возрастает и стоимость объекта, потому как в зомбированном состоянии стоимость объекта складывается из его основной стоимости, а также стоимости «зомби-сети». Глубина защищенности отражает в данном случае достаточный уровень защиты, на котором возможно полноценное управление объектом.

Специалистами американской фирмы IBM была предложена эмпирическая зависимость для оценки уязвимости [8]:

$$R_i = 10^{(S_i + V_i - 4)},$$

где  $S_i$  и  $V_i$  — коэффициенты, характеризующие возможную частоту возникновения угрозы и значение возможного ущерба при ее возникновении. Выбранные значения этих коэффициентов лежали каждый в отдельности в диапазоне от 0 до 7. Например, для угрозы, ожидаемой раз в неделю

<sup>2</sup> Нормальное состояние системы — это такое состояние, в котором значения параметров объекта устойчивы и обеспечивают полноценное функционирование системы.

<sup>3</sup> «Зомби-сеть» — компьютерная сеть, состоящая из компьютеров, зараженных одним классом вредоносных программ, и управляемых одной серверной частью вредоносных программ.

( $S_i=6$ ), и значения возможного ущерба около 300 тыс. р. ( $V_i=4$ ), значение уязвимости будет соответствовать  $10^6$ .

Можно также провести оценку информационных рисков атакуемого объекта для чего целесообразно использовать модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угрозу и уязвимость следует понимать как: угроза — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации; уязвимость — слабость в системе защиты, которая делает возможным реализацию угрозы [9].

Вероятность происшествия зависит от уровней (вероятностей) угроз и уязвимостей:

$$P_{\text{проис}} = P_{\text{угр}} \cdot P_{\text{уязв}}.$$

Подобаяющим образом риск определяется как:

$$\text{РИСК} = P_{\text{угр}} \cdot P_{\text{уязв}} \cdot \text{ЦЕНА\_ПОТЕРИ}.$$

Стоит отметить, что имеются практические сложности в реализации этого подхода, а именно необходимо проводить сбор весьма обширного материала о происшествиях в этой области, а также возможны ошибки при оценке угроз и уязвимостей при недостоверном либо недостаточном статистическом материале [10].

Однако не стоит думать, что отсутствуют меры противодействия киберпреступлениям, совершаемым с использованием вредоносных кодов. Согласно основным законам криминалистики (закон индивидуальности, отражения, накопления и закон всеобщей связи и взаимной обусловленности), после совершения киберпреступления с применением вредоносных кодов также остается множество следов, как материальных, так и идеальных [11].

К идеальным следам можно в данном случае отнести следы виртуального общения со злоумышленником посредством почтовых программ и сервисов мгновенных сообщений, например впечатление, сложившееся в переписке с клерком продуктовой компании, знакомого с тонкостями хакерского жаргона. К материальным следам относятся все сведения, зафиксированные на материальных носителях, например, журналы системных событий, событий безопасности и приложений, журналы подключений серверов, журналы работы внешних устройств и т. п. [12]. Но в случае киберпреступления, связанного с применением вредоносных кодов, имеется еще одна очень важная группа следов — непосредственно зараженные вредоносными кодами исполняемые файлы. Именно исследованием этих файлов можно установить не только «характер и поведение» вредоносной программы, но и ее отличительные особенности, такие как сетевые адреса злоумышленника, его кличку, его сетевой идентификатор в сети обмена мгновенными сообщениями и т. д.

Бывают и ситуации, когда объект еще только находится под атакой злоумышленника. В этом случае обнаружить его вторжения можно при помощи специализированных утилит по сбору сетевого трафика, файловых и процессовых мониторов, а также поиском в системных папках операционной системы упакованных объектов. В случае обнаружения подозрительной активности либо замаскированных процессов и объектов, необходимо принять адекватные меры противодействия.

Таким образом, имея модель киберпреступления, зная ее особенности и проводя описанные выше мероприятия, можно эффективно противодействовать киберпреступности, основанной на использовании вредоносных кодов.

## СПИСОК ЛИТЕРАТУРЫ

- Lewis J.A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. — Washington, D.C., 2003. [http://crime.vl.ru/docs/stats/stat\\_82.htm](http://crime.vl.ru/docs/stats/stat_82.htm)
- Shinder D.L. Scene of the Cybercrime: Computer Forensics Handbook, Chapter 1, Facing the Cybercrime Problem Head On, Center for Strategic and International Studies. — Washington, D.C., 2002. [http://crime.vl.ru/docs/stats/stat\\_68.htm](http://crime.vl.ru/docs/stats/stat_68.htm)
- Denning D.E. Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Georgetown University. — N.Y., 2001. [http://crime.vl.ru/docs/stats/stat\\_92.htm](http://crime.vl.ru/docs/stats/stat_92.htm)
- Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика. — М.: Гелиос АРВ, 2006. — 240 с.
- Макклуре С., Скембрэй Дж., Куртц Дж. Секреты хакеров, проблемы и решения сетевой защиты. — М.: ЛОРИ, 2001. — 435 с.
- Завгородний В.И. Комплексная защита информации в компьютерных системах. <http://eusi.narod.ru/lib/savgorodnij/>
- Гошко С.В. Энциклопедия по защите от вирусов. — М.: СОЛОН-Пресс, 2004. — 304 с.
- Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. — М.: Горячая линия-Телеком, 2006. — 350 с.
- Реализация концепции управления рисками на практике. <http://www.jetinfo.ru/2003/2/1/article1.2.2003197>
- Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. — М.: Гелиос АРВ, 2005. — 224 с.
- Усов А.И. Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем. — М.: Право и закон, 2002. — 384 с.
- Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники. — М.: ЦИ и НМОКП МВД России, 2000. — 64 с.