DOI: https://doi.org/10.15688/jvolsu10.2017.3.1

УДК 332(075.8)
ББК 65.422

ВОПРОСЫ РАБОТЫ С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ НА ЭТАПЕ РАССЛЕДОВАНИЯ

Елена Александровна Максимова

Кандидат технических наук, доцент,
заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Мария Викторовна Бердник

Доцент кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
ktib91@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Вадим Юрьевич Цыбанов

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Анна Викторовна Алексеенко

Лаборант кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе представлена разработанная модель злоумышленника, способного совершить компьютерное преступление. С целью реализации модели работы с компьютерными преступлениями на этапе расследования разработана архитектура, использованная в алгоритмической модели, позволяющей автоматизировать процесс работы с компьютерными преступлениями на этапе расследования.

Ключевые слова: компьютерные преступления, модель злоумышленника, архитектура модели, этап расследования, алгоритм действий.

В последнее время количество компьютерных преступлений постоянно увеличивается. Так, согласно данным, полученным из ГИАЦ МВД РФ [2], количество преступных посягательств за последние 10 лет возросло в 22,3 раза и продолжает увеличиваться в среднем в 3,5 раза ежегодно; ежегодный размер материального ущерба от рассматриваемых преступных посягательств составляет 613,7 млн рублей; средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен 1,7 млн рублей. В это же время с определенной долей успеха расследуется лишь около 49 % преступлений; обвинительные приговоры выносятся лишь в 25,5 % случаев от общего числа возбужденных уголовных дел; средний показатель количества уголовных дел, по которым производство приостановлено, составляет 43,5 % и ярко отражает низкую степень профессионализма сотрудников правоохранительных органов в деятельности по раскрытию, расследованию и предупреждению указанных преступных посягательств.

Так как при работе с компьютерными преступлениями до настоящего времени используются стандартные алгоритмы действий, не учитывающие специфик данного вида деяний, то это является одной из причин роста киберпреступности и низким показателем их раскрытия. Таким образом, необходим новый подход к работе с компьютерными преступлениями с учетом специфики преступления и модели потенциального злоумышленника, особенно на этапе расследования.

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д. [3].

В уголовно-правовой литературе используется целый ряд понятий: «информационное преступление», «компьютерное преступление», «преступление в сфере компьютерной информации». Первые два из них пересекаются. Предметом информационного преступления является любая информация, в том числе и компьютерная. Под компьютерным преступлением понимается предусмотренное уголовным законом общественно опасное действие, в котором машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления выступает машинная информация, компьютер, компьютерная система или компьютерная сеть [4; 9].

Одной из наиболее распространенных классификаций преступлений в сфере компьютерной информации является кодификатор рабочей группы Интерпола. Согласно данному кодификатору все компьютерные преступления классифицированы по следующим основным классам:

QA – Несанкционированный доступ и перехват.

QD – Изменение компьютерных данных.

QF – Компьютерное мошенничество.

QR – Незаконное копирование.

QS – Компьютерный саботаж.

QZ – Прочие компьютерные преступления [1].

Данная классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола.

Однако в ряде классификаций, как и в обозначенной, присутствует неоднозначность и неопределенность понятия «компьютерное преступление» из-за смешения уголовно-правовых начал и технических особенностей автоматизированной обработки информации.

В.А. Мещеряковым выделены следующие классы:

1-й класс. Неправомерное завладение информацией или нарушение исключительного права ее использования.

2-й класс. Неправомерная модификация информации.

3-й класс. Разрушение информации.

4-й класс. Действие или бездействие по созданию (генерации) информации с заданными свойствами.

5-й класс. Действия, направленные на создание препятствий пользования информацией законным пользователям [1].

Тем не менее в данной классификации отражены не преступления, а набор возможных противоправных посягательств на компьютерную информацию.

В соответствии с законодательством РФ компьютерные преступления классифицируются следующим образом: компьютерные преступления в сфере оборота компьютерной информации; в сфере телекоммуникаций; в сфере информационного оборудования; в сфере защиты охраняемой законом информации. Каждый вид компьютерных преступлений при этом рассматривается в ст. 129 УК РФ, ст. 137 УК РФ, 138 УК РФ, ст. 140 УК РФ, ст. 146 УК РФ, ст. 155 УК РФ, ст. 159 УК РФ, ст. 165 УК РФ, ст. 169 УК РФ, ст. 171, 171.1 УК РФ, 173 УК РФ, ст. 175 УК РФ, 178 УК РФ, ст. 182 УК РФ, ст. 183 УК РФ, ст. 185.1 УК РФ, ст. 186 УК РФ, ст. 187 УК РФ, ст. 189 УК РФ, ст. 194 УК РФ, ст. 198 УК РФ, ст. 199 УК РФ, ст. 200 УК РФ, ст. 237 УК РФ, ст. 242 УК РФ, ст. 272 УК РФ, ст. 273 УК РФ, ст. 274 УК РФ, ст. 276 УК РФ, ст. 283 УК РФ, ст. 287 УК РФ, ст. 310 УК РФ, ст. 311 УК РФ, ст. 320 УК РФ.

Кроме того, введены три федеральных закона, касающихся безопасности критической информационной инфраструктуры РФ, подписанных президентом 26 июля 2017 года. Так, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак [8]. Закон устанавливает принципы обеспечения безопасности критической информационной инфраструктуры. Определяются полномочия государственных органов РФ в области обеспечения ее безопасности, а также права и обязанности субъектов критической информационной инфраструктуры. Закон определяет функции Национального координационного центра по компьютерным инцидентам.

Помимо этого, опубликованы еще два федеральных закона, тесно связанных с первым. Один из них – «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"». Внесены изменения в Закон РФ «О государственной тайне», Федеральный закон «О связи» и в Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"» дополняет главу 28 («Преступления в сфере компьютерной информации») УК РФ специальной статьей 2741, предусматривающей ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, за неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, а также за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ [7].

Классически расследование компьютерных преступлений выполняется в соответствии со следующими этапами [6]:

1) допрос свидетеля и потерпевшего;
2) следственный осмотр;
3) обыск и выемка;
4) назначение и производство экспертизы;
5) следственный эксперимент;
6) допрос обвиняемого и подозреваемого.

При этом на этапе расследования в классическом виде у подозреваемого в ходе допроса выясняются его возможности, мотивация и т. д. То есть определяется возможность данного субъекта к совершению преступления.

Однако, имея дело с компьютерными преступлениями, мы предлагаем уже после

первых двух этапов расследования создать модель злоумышленника (инфомодель), что позволит повысить эффективность работы с компьютерными преступлениями с точки зрения оптимизации ресурсов.

Модель злоумышленника информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д. [5]. В таблице представлена разработанная инфомодель злоумышленника, способного совершить компьютерное преступление.

Инфомодель злоумышленника, способного совершить компьютерное преступление

№ п.п.	Тип нарушителя	Вид нарушителя	Мотивация *	Предположения о возможностях нарушителя	Вид компьютерного преступления
1	Внутренний	Сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР, но имеющие санкционированный доступ в КЗ	М4, М6	Располагает именами и ведет выявление паролей зарегистрированных пользователей; изменяет конфигурацию технических средств обработки; вносит программно-аппаратные закладки в ПТС и обеспечивает съем информации, используя непосредственное подключение к техническим средствам обработки информации	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
2	Внутренний	Зарегистрированные пользователи, осуществляющие ограниченный доступ к ИР с рабочего места	М1, М6, М7, М8	Обладает всеми возможностями лиц первой категории; знает, по меньшей мере, одно легальное имя доступа; обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ИР; располагает ПДн, к которым имеет доступ	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Непреднамеренные, неосторожные или неквалифицированные действия. Любопытство или желание самореализации. Месть за ранее совершенные действия
3	Внутренний	Зарегистрированные пользователи подсистем, осуществляющие удаленный доступ к ПДн по локальной или распределенной сети предприятий	М1, М2, М6, М7, М8	Обладает всеми возможностями лиц второй категории; располагает информацией о топологии сети и составе технических средств; имеет возможность прямого (физического) доступа к отдельным техническим средствам	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Непреднамеренные, неосторожные или неквалифицированные действия. Любопытство или желание самореализации. Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внутренний	Зарегистрированные пользователи с полномочиями администратора безопасности сегмента (фрагмента)	М5, М4, М6	Обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте; обладает полной информацией о технических средствах и конфигурации сегмента; имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте; имеет доступ ко всем техническим средствам сегмента; обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Непреднамеренные, неосторожные или неквалифицированные действия

Окончание таблицы

№ п.п.	Тип нарушителя	Вид нарушителя	Мотивация *	Предположения о возможностях нарушителя	Вид компьютерного преступления
5	Внутренний	Зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа	М4, М6	Обладает полной информацией о системном, специальном и прикладном программном обеспечении, используемом в сегменте; обладает полной информацией о технических средствах и конфигурации сегмента; имеет доступ ко всем техническим средствам и данным; обладает правами конфигурирования и административной настройки технических средств	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
6	Внешний	Бывшие сотрудники	М1, М8	Обладает всеми возможностями лиц второй категории; располагает информацией о топологии сети и составе технических средств; имеет возможность прямого (физического) доступа к отдельным техническим средствам	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия
7	Внешний	Посторонние лица, пытающиеся получить доступ к конфиденциальной информации в инициативном порядке	М1, М2, М7, М9	Располагает именами и ведет выявление паролей зарегистрированных пользователей; изменяет конфигурацию технических средств обработки; вносит программно-аппаратные закладки в ПТС и обеспечивает съем информации, используя непосредственное подключение к техническим средствам обработки информации	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации. Идеологические или политические мотивы
8	Внешний	Представители преступных организаций	М1, М2	Обладает всеми возможностями лиц первой категории; знает, по меньшей мере, одно легальное имя доступа; обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР; располагает ПДн, к которым имеет доступ	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды

Примечание. * Возможные цели (мотивация) реализации угроз безопасности информации: *М1* – причинение имущественного ущерба путем мошенничества или иным преступным путем; *М2* – выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды; *М3* – получение конкурентных преимуществ; *М4* – причинение имущественного ущерба путем обмана или злоупотребления доверием; *М5* – внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки; *М6* – непреднамеренные, неосторожные или неквалифицированные действия; *М7* – любопытство или желание самореализации (подтверждение статуса); *М8* – месть за ранее совершенные действия; *М9* – идеологические или политические мотивы.

На основании вышеизложенного можно представить функцию работы с компьютерными преступлениями на этапе расследования в виде

$$F = F(VK, F_1) = F(VK(T, V, C), F_1),$$

где T – множество исходных данных; V – множество типичных ситуаций; C – множество рекомендованных следственных действий; VK – множество видов компьютерных преступлений; F_1 – функция инфомодели (модели злоумышленника).

Причем в зависимости от постановки задачи возможны варианты:

$$VK = VK(F_1) \text{ или } F_1 = F_1(VK).$$

Сама же функция инфомодели (модели злоумышленника) примет вид:

$$F_1 = F_1(\text{Тн}, \text{М}, \text{Вн}).$$

где Тн – множество типов злоумышленника; М – множество мотиваций для злоумышленных воздействий; Вн – множество возможностей злоумышленника.

То есть

$$F_1 = F_1(F(VK(T, V, C))).$$

С целью реализации модели работы с компьютерными преступлениями на этапе расследования разработана архитектура (см. рисунок), использованная в алгоритмической модели, позволяющей автоматизировать процесс работы с компьютерными преступлениями на этапе расследования.

СПИСОК ЛИТЕРАТУРЫ

1. Виды компьютерных преступлений. – Электрон. дан. – Режим доступа: https://studfiles.net/preview/4395500/page:3. – Загл. с экрана.

2. Главный информационно-аналитический центр Министерства внутренних дел РФ. – Электрон. дан. – Режим доступа https://мвд.рф/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen. – Загл. с экрана.

3. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности : дата введения 2006-06-01. Ч. 1 // Консорциум «Кодекс». Электронный фонд правовой и нормативно-технической документации. – Режим доступа: http://docs.cntd.ru/document/1200048398. – Загл. с экрана. – Подготовлен АО «Кодекс» и сверен по: официальное издание, М. : Стандартинформ, 2007.

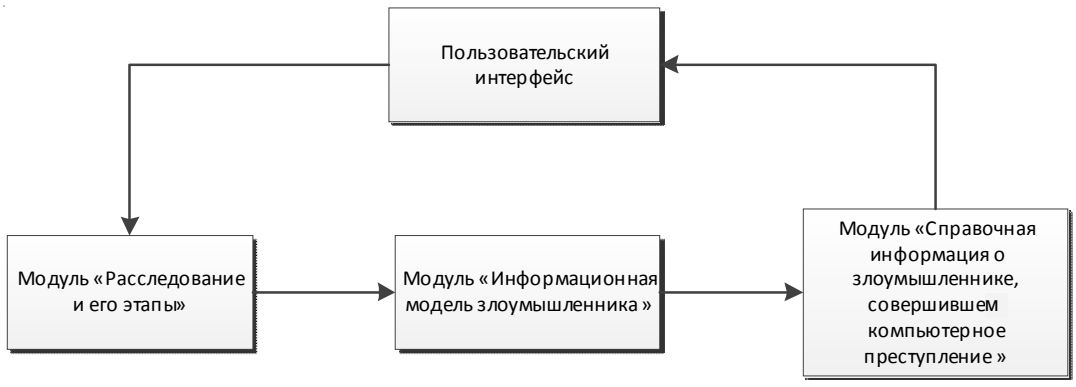
4. Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – М. : Новый Юрист, 1998.

5. Модель нарушителя информационной безопасности // Студопедия. – Электрон. дан. – Режим доступа: https://studopedia.ru/2_37113_model-narushitelya-informatsionnoy-bezopasnosti.html. – Загл. с экрана.

6. Расследование преступления в компьютерной сфере // www.Grandars.ru : [сайт]. – Электрон. дан. – Режим доступа: http://www.grandars.ru/college/pravovedenie/r-kompyuternyh-prestupleniy.html. – Загл. с экрана.

7. УК РФ. Статья 273. Создание, использование и распространение вредоносных компьютерных программ. – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/. – Загл. с экрана.

8. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной



Архитектура реализации модели работы с компьютерными преступлениями на этапе расследования

инфраструктуры Российской Федерации». – Электрон. дан. – Режим доступа: http://www.garant.ru/hotlaw/federal/1125425/. – Загл. с экрана.

9. The analysis of methods and approaches for modeling components of the complex organizational and technical systems “smart city” / Yu. S. Bakhracheva, A. A. Kadyrov, A. A. Kadyrova, E. A. Maksimova // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 6–10. – DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

REFERENCES

1. *Vidy kompyuternykh prestupleniy* [Types of Computer Crimes]. URL: https://studfiles.net/preview/4395500/page:3.

2. *Glavnyy informatsionno-analiticheskiy tsentr Ministerstva vnutrennikh del RF* [The Main Information-Analytical Center of the Ministry of Interior of the Russian Federation]. URL: https://mvd.rf/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen.

3. GOST R ISO/MEK 13335-1-2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti: data vvedeniya 2006-06-01. Ch. 1 [GOST R ISO/MEK 13335-1-2006. Information Technology. Methods and Means of Providing Security. Adoption Date – June 1, 2006. Part 1]. *Konsortsium «Kodeks». Elektronnyy fond pravovoy i normativno-tekhnicheskoy dokumentatsii* [Consortium “Codex”. Electronic Fund of Legal and Regulatory Technical Documentation]. URL: http://docs.cntd.ru/document/1200048398.

4. Kurushin V.D., Minaev V.A. *Kompyuternye prestupleniya i informatsionnaya bezopasnost* [Computer Crimes and Information Security]. Moscow, Novyy yurist Publ., 1998

5. Model narushitelya informatsionnoy bezopasnosti [Model of Information Security Offender]. *Studopediya*. URL: https://studopedia.ru/2_37113_model-narushitelya-informatsionnoy-bezopasnosti.html.

6. *Rassledovanie prestupleniya v kompyuternoy sfere* [Investigation of Crimes in Computer Sphere]. URL: http://www.grandars.ru/college/pravovedenie/r-kompyuternyh-prestupleniy.html.

7. *UK RF. Statya 273. Sozdanie, ispolzovanie i rasprostranenie vredonosnykh kompyuternykh programm* [The Criminal Code of the Russian Federation. Article 273. The Creation, Use and Distribution of Malicious Computer Programs]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/.

8. *Federalnyy zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii»* [Federal Law of July 26, 2017 no. 187-FL “About the Security of Critical Information Infrastructure of the Russian Federation”]. URL: http://www.garant.ru/hotlaw/federal/1125425/.

9. Bakhracheva Yu.S., Kadyrov A.A., Kadyrova A.A., Maksimova E.A. The analysis of methods and approaches for modeling components of the complex organizational and technical systems “smart city”. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Technology and Innovations], 2017, vol. 11, no. 2, pp. 6-10. DOI: https://doi.org/10.15688/jvolsu10.2017.2.1.

INVESTIGATION OF COMPUTER CRIMES

Elena Aleksandrovna Maksimova

Candidate of Technical Sciences, Associate Professor,
Head of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky,100, 400062 Volgograd, Russian Federation

Mariya Viktorovna Berdnik

Associate Professor, Department of Computer Technologies and Information Security,
Kuban State Technological University
ktib91@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Vadim Yurevich Tsybanov

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky,100, 400062 Volgograd, Russian Federation

Anna Viktorovna Alekseenko

Laboratory Assistant, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky,100, 400062 Volgograd, Russian Federation

Abstract. In recent years, the number of computer crimes is constantly increasing. The number of criminal attacks over the last 10 years has increased by 22.3 % and continues to increase, on the average, in 3.5 times a year. The annual damage caused by this criminal assault amounts to 613,7 million roubles; the average damage from one computer to the victim of a crime is equal to 1.7 million roubles. At the same time, only about 49 % are successfully solved. Guilty verdicts are rendered only in 25.5 % cases from the total number of criminal cases. The average number of criminal cases, in which production is suspended, is 43.5 % and clearly reflects the low degree of professionalism of law enforcement bodies in the activities of disclosure, investigation and prevention of these criminal attacks.

Since standard algorithms of actions not taking into account the specificities of this type of criminal conduct are used when working with the computer crimes, we observe the growth of cybercrime and the low rate of disclosure. Thus, a new approach is necessary for investigating computer crimes, taking into account the specifics of the crime and modeling a potential attacker, especially at the stage of investigation.

Model intruder information security is a set of assumptions about one or more possible offenders of information security, their qualifications, their technical and material means, etc.

The paper presents the developed model of the attacker capable of committing a computer crime. The authors work out the architecture used in the algorithmic model allowing to automate the process of computer crimes investigation.

Key words: computer crimes, model of attacker, architecture of model, investigation stage, the algorithm of actions.