УДК 004.056.53 DOI: 10.17587/it.24.339-344

К. А. Щеглов, аспирант, e-mail: skd@npp-itb.spb.ru,
А. Ю. Щеглов, д-р техн. наук, проф., e-mail: info@npp-itb.spb.ru,
Университет ИТМО, Санкт-Петербург, Россия

Моделирование угроз целевых атак

Рассматривается подход к моделированию угроз целевых атак, отличающихся использованием потенциальными нарушителями при осуществлении атаки уязвимостей "нулевого дня". Эта особенность угрозы принципиально меняет задачу моделирования, поскольку в данном случае в модели уже отсутствует параметр интенсивности устранения уязвимости — она не устраняется, так как об уязвимости нулевого дня еще не известно разработчику уязвимого программного средства. Обсуждается, как учесть эту особенность угрозы атаки в математической модели, и какие количественные характеристики (мера) актуальности угрозы атаки при этом могут быть определены.

Ключевые слова: *угроза атаки, целевая атака, актуальность, количественная мера, математическое моделирование*

Введение

Основной проблемой современной информационной безопасности становятся целевые атаки. Это обусловлено тем, что несмотря на пока небольшой (порядка 1 %) процент от общего числа атак, нанесенный ущерб от целевых атак уже во много раз превосходит ущерб от массовых атак [1—4].

Целевые (или таргетированные) атаки — это атаки, направленные на конкретные коммерческие организации или государственные ведомства в целях получения несанкционированного доступа к информации. Такие атаки не носят массовый характер и готовятся достаточно длительный период [1—4].

В отличие от массовых атак компьютерных вирусов (цель которых — заражение максимального числа компьютеров), подобные атаки тщательно планируются, а вредоносное программное обеспечение специально разрабатывается для каждой атаки, чтобы антивирусы и иные средства защиты, используемые в информационной системе, не смогли обнаружить атаку. Как правило, для реализации целевой атаки используются уязвимости нулевого дня, не известные и не устраняемые на момент осуществления атаки.

Таким образом, основу целевой атаки составляет использование уязвимостей реализации программных средств (ошибок программирования, общая классификация угроз уязвимостей представлена в работе [5]), о которых еще кому-либо, кроме потенциального нарушителя, не известно.

Общий подход к математическому моделированию угрозы атаки как случайного процесса возникновения и устранения реальной угрозы (все создающие ее уязвимости выявлены, но еще не устранены) изложен в работе [5]. Уточним понятие "резервирование по угрозам уязвимостей" (или угроз уязвимостей). Именно возникновение в системе уязвимости позволяет реализовать атаку, т. е. угроза атаки создается угрозой возникновения в системе уязвимости (угрозой уязвимости). В общем случае для реализации атаки злоумышленнику может потребоваться воспользоваться несколькими разнородными, в том числе возникшими в различных средствах, одновременно присутствующими в системе уязвимостями. Вероятность такого события и, как следствие, актуальность угрозы такой атаки, естественно, будут ниже. Это позволяет интерпретировать угрозу атаки схемой параллельного резервирования (горячий резерв) создающих ее угроз уязвимостей, так как отказ безопасности системы, позволяющий реализовать атаку, возникает только при условии одновременного присутствия в системе всех уязвимостей, угрозы которых создают угрозу атаки. Если хотя бы одной уязвимости не возникнет, то реализация атаки будет невозможна. При этом соответствующим образом может интерпретироваться и задача построения системы защиты — система защиты должна обеспечивать невозмож-

ность осуществления атаки, без возникновения соответствующей уязвимости и непосредственно в системе защиты. Как видим, при такой интерпретации построения системы защиты угрозой уязвимости системы защиты, без возникновения которой невозможна атака, резервируются угрозы уязвимостей защищаемой системы [5].

Рассмотрим, как можно учесть при моделировании угрозы атаки тот факт, что атакой используется уязвимость нулевого дня, устранение которой до момента успешной реализации атаки не осуществляется.

1. Моделирование угроз массовых атак

Как отмечалось выше, в работе [5] изложены и обоснованы общие подходы к моделированию угроз атак и рассмотрены вопросы моделирования угроз массовых атак. Подход к моделированию проиллюстрируем на примере угрозы атаки, создаваемой угрозами уязвимостей двух типов. При этом моделируется марковский случайный процесс с дискретными состояниями и непрерывным временем. Искомые стационарные вероятности находятся решением соответствующей системы линейных уравнений [5]. Модель приведена на рис. 1.

Здесь λ_1, μ_1, λ_2, μ_2 — соответственно параметры угроз уязвимостей первого и второго типов — их интенсивности возникновения и устранения, значения которых могут определяться с использованием соответствующей статистики.

Состояния системы обозначены S_{ij}, где S_{00} — состояние, характеризуемое отсутствием уязвимостей в системе; S_{10} — состояние, характеризуемое присутствием в системе уязвимости первого типа; S_{01} — состояние, характеризуемое присутствием в системе уязвимости второго типа; S_{11} — состояние, характеризуемое присутствием в системе уязвимости первого и уязвимости второго типов — состояние реальной угрозы атаки.

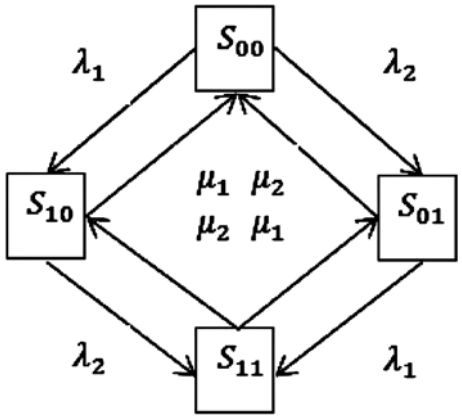

Рис. 1. Размеченный граф системы состояний случайного процесса угрозы массовой атаки

Моделируется стационарный режим, в результате моделирования определяются значения искомых параметров — интенсивности возникновения и устранения реальной (для реализации) угрозы атаки — и характеристик — стационарной вероятности готовности системы к безопасной эксплуатации, среднее время наработки системы на отказ безопасности и среднее время восстановления безопасности системы (в данном случае в отношении угрозы атаки). Таким образом, без использования каких-либо экспертных оценок может быть получена всесторонняя количественная оценка актуальности угрозы массовой атаки.

Рассмотрим особенности угрозы массовой атаки, учитываемые при построении соответствующих математических моделей. В данных моделях предполагается, что возникшая уязвимость программного средства сразу начинает устраняться его разработчиком, проще говоря, о возникшей уязвимости потенциальные нарушители (причем массово) и разработчик программного средства узнают практически одновременно. При этом потенциальный нарушитель может осуществить соответствующую атаку на информационную систему в промежутке времени с момента возникновения реальной угрозы атаки, о которой стало известно, до тех пор, пока она не будет соответствующим образом устранена, т. е. пока не будут сделаны исправления и соответствующие обновления программного средства (средств) не будут установлены в информационной системе.

2. Моделирование угроз эксклюзивных и гибридных целевых атак

Угроза атаки, относимая нами к разряду эксклюзивных целевых, характеризуется совсем иным образом. Принципиально подобная атака отличается тем, что при ее реализации используются уязвимости, известные только потенциальному нарушителю и не известные разработчику. При этом подобная угроза целевой атаки после первой же ее реализации становится угрозой массовых атак, так как об использованных при реализации атаки уязвимостях становится известно.

Принципиальным отличием предложенного подхода к моделированию эксклюзивной целевой атаки, проводимого в целях оценки ее актуальности, состоит в том, что в данном случае следует говорить о моделировании невосстанавливаемой системы — о невосстанавливаемом отказе безопасности. Это обусловливается тем, что возникающие уязвимости в программных средствах (их отказы безопасности) в данном случае

не устраняются, поскольку о них известно только потенциальному нарушителю.

Таким образом, для моделирования эксклюзивной целевой атаки может использоваться основной (или экспоненциальный) закон надежности, позволяющий в рамках теории надежности моделировать невосстанавливаемые отказы. В данном случае характеристикой угрозы атаки уже является среднее время наработки информационной системы до отказа безопасности.

Однако для получения возможности моделирования частично эксклюзивной (или гибридной) целевой атаки, о чем будет сказано далее, в данном случае также целесообразно построение соответствующей марковской модели угрозы атаки, при этом в качестве состояний системы должны использоваться невозвратные и поглощающее состояния (моделируется нестационарный режим).

Пример такой модели приведен на рис. 2, *а*.

Модель построена в предположении о том, что угроза атаки создается угрозами уязвимостей двух типов.

В модели, приведенной на рис. 2, *а*, S_{11} — это поглощающее состояние, после перехода в которое процесс завершается (стационарные вероятности для такой модели отсутствуют).

Состояния же S_{00}, S_{10}, S_{01} — невозвратные, характеризуются соответствующим средним временем пребывания в них системы T_{00}, T_{10}, T_{01}. Угроза атаки в соответствии с этой моделью невосстанавливаемой системы характеризуется средним временем наработки системы до отказа безопасности $T_{\text{но}}$, определяемым как

$$T_{\text{но}} = T_{00} + T_{10} + T_{01}.$$

Для построения искомой системы линейных уравнений можно использовать преобразование Лапласа — здесь уже необходимо определять не стационарные вероятности (система не стационарна), а временные характеристики — среднее время пребывания системы в соответствующих состояниях, а можно исходить из несколько иной интерпретации модели, представленной в работе [5]: n_i — это среднее число возникших уязвимостей i-го типа, переводящее систему из некоего состояния S_{rd}, определяемое как $n_i = \lambda_i T_{rd}$, где T_{rd} — среднее время пребывания системы в состоянии S_{rd}. Этими значениями взвешиваются дуги в графе переходов состояний, указывая на то, сколько в среднем переходов будет осуществлено из соответствующего состояния под воздействием какого-либо входного потока случайных событий.

При подобной интерпретации модели достаточно просто могут быть определены все искомые уравнения. Первое получаем исходя из того, что из состояния S_{00} будет осуществлен только один переход:

$$T_{00}(\lambda_1 + \lambda_2) = 1.$$

Среднее число переходов, переводящих систему в состояния S_{10} и S_{01} и переводящих систему из этих состояний, должно соответствующим образом совпадать, из чего получаем необходимые нам уравнения:

$$T_{00}\lambda_1 = T_{01}\lambda_2;$$
$$T_{00}\lambda_2 = T_{10}\lambda_1.$$

Этих уравнений достаточно для получения решения. Последнее же уравнение для модели, приведенной на рис. 2, *а*, на основе того, что в состояние S_{11} может быть осуществлен только один переход, имеет вид

$$T_{01}\lambda_2 + T_{10}\lambda_1 = 1.$$

Решая полученную систему линейных уравнений, определяем характеристику среднего времени наработки до отказа безопасности $T_{\text{но}}$ для модели, представленной на рис. 2, *а*:

$$T_{\text{но}} = \frac{1}{(\lambda_1 + \lambda_2)}\left(1 + \frac{\lambda_1}{\lambda_2} + \frac{\lambda_2}{\lambda_1}\right).$$

На практике более вероятны целевые атаки, отличающиеся тем, что потенциальному нарушителю известны уязвимости нулевого дня не для всех типов уязвимостей, создающих угрозу атаки. Назовем та-

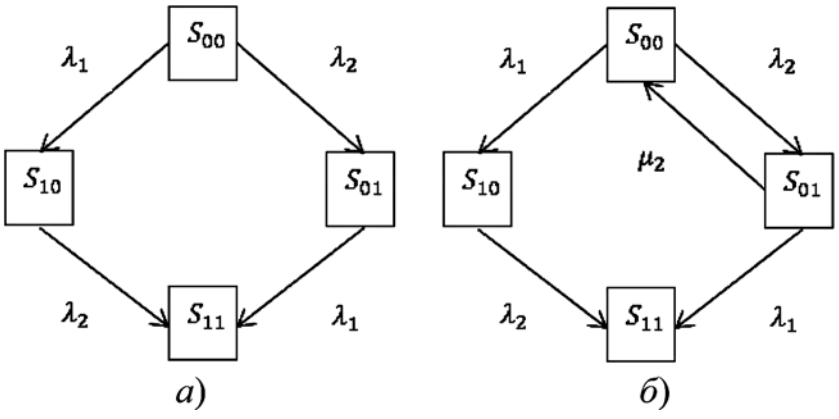

Рис. 2. Иллюстрация моделей угроз целевых атак:
а — эксклюзивная; *б* — гибридная

кие угрозы атак частично эксклюзивными или гибридными. Понятно, что такая целевая атака возможна в том случае, если угроза атаки создается угрозами уязвимостей нескольких типов.

Подобную угрозу целевой атаки с использованием предложенного подхода также можно промоделировать, пример модели подобной угрозы атаки приведен на рис. 2, *б*. В данном случае опять же моделируется невосстанавливаемая система в целом, однако при моделировании события возникновения используемых при реализации атаки известных (устраняемых) уязвимостей (для модели, приведенной на рис. 2, *б*, это уязвимости второго типа) уже используются сообщающиеся состояния: S_{00}, S_{01}.

Требуемые линейные уравнения опять же при этом могут быть получены с использованием рассмотренной ранее интерпретации переходов между состояниями. Например, с учетом того, что из состояния S_{00} число переходов будет на 1 больше, чем число возвратов в это состояние, первое уравнение будет иметь следующий вид:

$$T_{00}(\lambda_1 + \lambda_2) - T_{01}\mu_2 = 1.$$

По аналогии с тем, как это было сделано ранее, можно построить и остальные требуемые уравнения.

Решение данной задачи моделирования позволяет количественно определять то, насколько изменится актуальность угрозы атаки в том случае, если нарушителем частично при реализации атаки будут использоваться новые неизвестные кому-либо уязвимости.

Таким образом, данный метод моделирования для оценки актуальности угрозы целевой атаки заключается в моделировании невосстанавливаемого отказа безопасности системы в отношении этой угрозы, что учитывается в модели использованием поглощающего состояния. При этом, поскольку в такой модели отсутствует стационарный режим, моделируется временная характеристика безопасности — среднее время наработки системы до отказа безопасности.

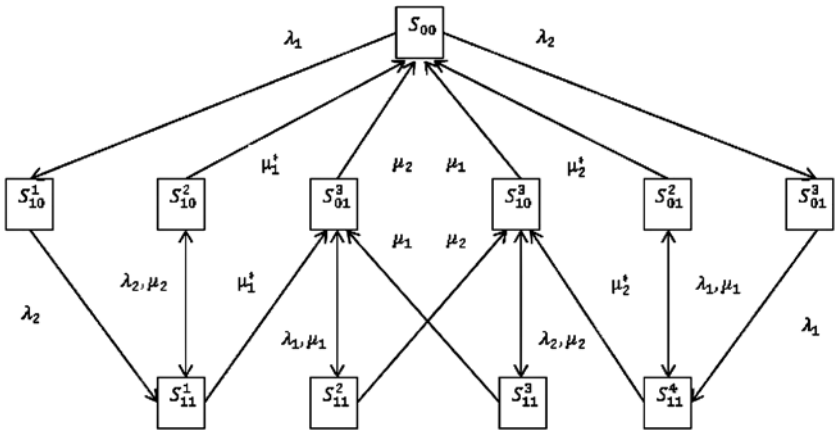

Рис. 3. Иллюстрация модели угрозы атаки в общем виде

3. Моделирование угроз атак в общем виде

В общем случае с учетом возникновения и устранения уязвимостей в процессе работы системы угроза атаки может принимать различные формы, что можно соответствующим образом учесть при ее моделировании, более корректно описав угрозу целевой атаки. Будем рассматривать далее угрозу атаки в общем виде — с учетом ее трансформации в процессе функционирования системы, при условии, что угроза атаки создается угрозами уязвимостей нескольких типов.

Так, изначально при отсутствии уязвимостей их возникновение создает реальную угрозу эксклюзивной целевой атаки. Далее, когда все возникшие уязвимости одного типа будут устранены, а другого типа еще нет, возникновение новой уязвимости того типа, все уязвимости которого были устранены, уже создает реальную угрозу гибридной атаки, поскольку данная уязвимость нулевого дня сразу может быть использована для осуществления атаки, угроза которой становится реальной. Наличие же в системе одновременно уязвимостей всех типов, создающих угрозу атаки, о которых известно, которые устраняются, создает уже реальную угрозу массовой атаки.

Рассмотрим, как подобное изменение формы, принимаемой угрозой атаки в процессе функционирования системы, может быть учтено при моделировании путем построения модели угрозы атаки в общем виде, опять же в предположении о том, что угроза атаки создается угрозами уязвимостей двух типов, которая приведена на рис. 3. Можно говорить, что это модель угрозы атаки в общем виде, поскольку ею учитываются все формы, принимаемые угрозой атаки в процессе функционирования системы.

Поскольку в данном случае нас будет интересовать случайный процесс изменения формы угрозы целевой атаки, и при этом все уязвимости должны устраняться, естественно, строим модель восстанавливаемой системы, позволяющей определять соответствующие параметры, вероятностные и временные характеристики угрозы атаки для стационарного режима функционирования системы.

Состояние S_{00} в модели — это состояние, характеризующее отсутствие

уязвимостей в системе, S_{10}^{i} — состояния, характеризующие присутствие в системе, по крайней мере, одной уязвимости первого типа, S_{01}^{i} — состояния, характеризующие присутствие в системе, по крайней мере, одной уязвимости второго типа, S_{11}^{j} — состояния, характеризующие присутствие в системе, по крайней мере, одной уязвимости первого типа и, по крайней мере, одной уязвимости второго типа, угроза атаки в этих состояниях реальна.

Отметим, что данная модель соответствует неразложимой непериодической цепи Маркова с конечным числом состояний, как следствие, она имеет стационарный режим функционирования и может характеризоваться соответствующими финальными вероятностями состояний.

Рассмотрим данную модель, при этом поясним, почему потребовалось ввести в модель i состояний S_{10} и S_{01} и j состояний S_{11}, и определимся с тем, как и в результате чего меняется форма целевой атаки. Анализ модели будем проводить исходя из того, что система осуществляет переход $S_{00} \to S_{10}^{1}$ (в случае перехода $S_{00} \to S_{01}^{3}$ анализ проводится полностью аналогично).

Переход $S_{00} \to S_{10}^{1}$ предполагает возникновение уязвимости нулевого дня первого типа, при этом данная уязвимость потенциальным нарушителем не используется (ему неизвестна уязвимость второго типа). При нахождении системы в состоянии S_{10}^{1} может возникнуть несколько уязвимостей первого типа (имеем угрозу отказа безопасности [5]), что требуется учесть в модели. Переход $S_{10}^{1} \to S_{11}^{1}$ предполагает возникновение реальной эксклюзивной угрозы целевой атаки, которая будет реализована, в результате чего об уязвимостях нулевого дня каждого типа становится известно, они начинают устраняться. В результате этого угроза атаки становится массовой. В это время могут возникать новые уязвимости обоих типов, появление которых повлияет на продолжение пребывания системы в состоянии S_{11}^{1}. При возникновении же новой возникшей уязвимости нулевого дня какого-либо типа при пребывании системы в состоянии S_{11}^{1} угроза этой целевой атаки становится гибридной. В зависимости от того, все возникшие уязвимости какого типа будут устранены раньше, система из состояния S_{11}^{1} перейдет в состояние S_{10}^{2}, либо в состояние S_{01}^{3}. И так далее.

Теперь рассмотрим, с какой целью, кроме состояния S_{10}^{2}, дополнительно в модель включено состояние S_{10}^{3}. Это обусловлено различными интенсивностями (интенсивность восстановления отказа безопасности [5]) возврата системы из этих состояний, соответственно, μ_1 и μ_1^*. Интенсивностью μ_1^* учитывается то, что при нахождении системы в состоянии S_{10}^{1} может возникнуть несколько уязвимостей первого типа нулевого дня, при этом необходимо учесть устранение их всех в системе. В состоянии S_{10}^{1} эти уязвимости не устраняются, так как их устранение начинается после осуществления эксклюзивной целевой атаки, когда о них становится известно. Устраняются эти уязвимости при нахождении системы в состояниях S_{10}^{2} и S_{11}^{1}, что учитывается использованием интенсивности μ_1^*. Переход же $S_{01}^{3} \to S_{11}^{2}$ предполагает, что все накопленные ранее уязвимости нулевого дня первого типа в состоянии S_{10}^{1} и уязвимости этого типа, возникшие при пребывании системы в состоянии S_{11}^{1}, устранены, поэтому для перехода $S_{01}^{3} \to S_{00}$ уже учитывается интенсивность μ_1 (интенсивность устранения уязвимости).

Используем для обозначения стационарных вероятностей состояний те же индексы, что и для обозначения соответствующих состояний.

В предположении о том, что накопления уязвимостей в состоянии S_{10}^{1} не происходит, исходя из стационарности режима функционирования системы можем записать:

$$P_{10}^{1}\lambda_2 + (P_{10}^{2} + P_{11}^{1})\lambda_1 = (P_{10}^{2} + P_{11}^{1})\mu_1.$$

Если же мы учтем накопление уязвимостей в состоянии S_{10}^{1}, которые должны быть устранены при нахождении системы в состояниях S_{10}^{2} и S_{11}^{1}, то соответственно получим

$$P_{10}^{1}\lambda_2 + (P_{10}^{2} + P_{11}^{1} + P_{10}^{1})\lambda_1 = (P_{10}^{2} + P_{11}^{1})\mu_1,$$

откуда μ_1^* можем определить следующим образом:

$$\mu_1^* = \mu_1 - \frac{P_{10}^{1}\lambda_1}{P_{10}^{2} + P_{11}^{1}}.$$

Аналогично для μ_2^* можем записать:

$$\mu_2^* = \mu_2 - \frac{P_{01}^{3}\lambda_2}{P_{01}^{2} + P_{11}^{4}}.$$

Построив подобную модель, уже можно рассчитать все искомые параметры и характеристики угрозы целевой атаки в общем виде с учетом различных принимаемых ею форм в процессе функционирования информационной системы: интенсивности возникновения в системе отказов безопасности (по крайней мере, одной реальной угрозы атаки) λ_a, интенсивность устранения в системе отказов безопасности (всех одновременно присутствующих реальных угроз атак) μ_a, вероятность готовности системы к безопасной эксплуатации P_{0a}, среднее время наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки

T_o, среднее время восстановления безопасности информационной системы $T_в$ в отношении угрозы атаки, что позволит корректно количественно оценить уровень ее актуальности. Например, для модели, приведенной на рис. 3, имеем:

$$P_{0a} = 1 - P_{11}^1 - P_{11}^2 - P_{11}^3 - P_{11}^4;$$

$$\lambda_a = (P_{01}^1 + P_{01}^2 + P_{01}^3)\lambda_1 + (P_{10}^1 + P_{10}^2 + P_{10}^3)\lambda_2;$$

$$\mu_a = \frac{(P_{01}^1 + P_{01}^2 + P_{01}^3)\lambda_1 + (P_{10}^1 + P_{10}^2 + P_{10}^3)\lambda_2}{P_{11}^1 + P_{11}^2 + P_{11}^3 + P_{11}^4};$$

$$T_в = \frac{1}{\mu_a},\ T_o = \frac{1}{\lambda_a} - T_в.$$

Кроме того, данная модель позволяет получить и ряд иных важных параметров и характеристик, уже связанных с изменением формы угрозы атаки в процессе функционирования системы. Например, интенсивность $\lambda_{ца}$ возникновения в системе реальных угроз эксклюзивной целевой атаки, предполагающей использование уязвимостей нулевого дня, можно для модели, приведенной на рис. 3, определить следующим образом:

$$\lambda_{ца} = P_{10}^1\lambda_2 + P_{01}^3\lambda_1,$$

интенсивность же $\lambda_{гца}$ возникновения в системе реальных угроз гибридной целевой атаки:

$$\lambda_{гца} = (P_{10}^2 + P_{10}^3)\lambda_2 + (P_{01}^2 + P_{01}^3)\lambda_1.$$

Таким образом, предложенный подход к моделированию позволяет определять все требуемые параметры и характеристики угрозы целевой атаки, позволяющие количественно оценивать уровень ее актуальности, с учетом всех этапов ее трансформации.

Список литературы

1. **Рынок** ищет способы защиты от целевых атак. URL:/http://www.cnews.ru/reviews/security2014/articles/rynok_ishchet_sposoby_zashchity_ot_tselevyh_atak, свободный (02.04.2017).

2. **Таргетированные** атаки и как с ними бороться. URL:/ https://www.iemag.ru/analitics/detail.php?ID=32831, свободный (02.04.2017).

3. **Целевые** атаки (APT). URL:/ https://www.anti-malware.ru/threats/target-attack, свободный (02.04.2017).

4. **Целевые** атаки — угроза номер один. Вестник цифровой трансформации CIO.RU. URL:/ http://www.cio.ru/articles/724, свободный (02.04.2017).

5. **Щеглов А. Ю., Щеглов К. А.** Защита информации: основы теории: учебник для бакалавриата и магистратуры. М.: Издательство Юрайт, 2017. 309 с.

K. A. Shcheglov, Postgraduate Student, skd@npp-itb.spb.ru,
A. Yu. Shcheglov, D. Sc., Professor, info@npp-itb.spb.ru,
ITMO University, St. Petersburg, 197101, Russian Federation

Targeted Attacks Threat Modeling

In this article is dedicated to targeted attacks threat modeling approach, which is marked by use of zero-day vulnerabilities by the potential intruder. This feature radically changes the task of modeling, because of software tools vulnerabilities threat reservation absence in such case (which means a system without reservation must be modeled). Security breakups in this case are not managed because of their unknown status (only the potential intruder knows about this vulnerabilities). In common case taking in mind vulnerabilities appearing and eliminating during system work, attack threat can be present in different forms, which needs to be taken into account while threat modeling (making targeted attack threat description more correct). At the beginning threat is known only by potential intruder, then after it's identification the process of threat eliminating begins. After such process system became restorable, which needs to be taken into account while attack threat modeling (attack can turn it's form). In common case while attack implementation potential intruder can use both unknown and known vulnerabilities which create attack threat meanwhile known vulnerability is not yet patched. Let's review how to calculate these attack threat features inside the mathematical model and which attack threat actuality characteristics (measures) can be defined. We will use Markov model with discrete state and continues time to build attack threat model. The suggested targeted attacks threat modeling approach has such advantages as ability to receive actuality quantitate measures without using of any subjective expert decisions.

Keywords: *attack threat, targeted attack, actuality, quantitate measure, mathematical modeling*

References

1. ***Rynok*** *ishchet sposoby zashchity ot celevyh atak,* available at: http://www.cnews.ru/reviews/security2014/articles/rynok_ishchet_sposoby_zashchity_ot_tselevyh_atak, svobodnyj (date of access: 02.04.2017).

2. ***Targetirovannye*** *ataki i kak s nimi borot'sya*, available at: https://www.iemag.ru/analitics/detail.php?ID=32831, svobodnyj (02.04.2017).

3. ***Celevye*** *ataki (APT),* available at: https://www.anti-malware.ru/threats/target-attack, svobodnyj (02.04.2017).

4. ***Celevye*** *ataki — ugroza nomer odin. Vestnik tsifrovoi transformatsii* CIO.RU, available at: http://www.cio.ru/articles/724, svobodnyj (02.04.2017).

5. **Shcheglov A. Yu., Shcheglov K. A.** *Zashchita informacii: osnovy teorii: uchebnik dlya bakalavriata i magistratury* (Information security: base theory: bachelor and magister materials), Moscow, Yurajt, 2017, 309 p. (in Russian).