ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.056.53
DOI: 10.17586/0021-3454-2015-58-12-957-965

МАРКОВСКИЕ МОДЕЛИ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

К. А. Щеглов, А. Ю. Щеглов

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: info@npp-itb.spb.ru

Исследованы принципиальные различия в постановке и решении задач моделирования характеристик надежности и безопасности информационных систем, с учетом которых построены марковские модели угрозы безопасности информационной системы. Обоснована корректность использования марковских процессов при моделировании характеристик безопасности информационных систем. Обоснована необходимость рассмотрения при моделировании характеристик безопасности в качестве элемента безопасности не угрозы атаки, а угрозы уязвимости. Разработаны марковская и укрупненная марковская модели безопасности информационной системы, а также формальная модель нарушителя, которые могут использоваться при проектировании системы защиты информационной системы.

Ключевые слова: *информационная система, информационная безопасность, угроза уязвимости, угроза атаки, угроза безопасности информационной системы, моделирование, марковский процесс, марковская модель, характеристика безопасности.*

Введение. В работах [1, 2] было предложено рассматривать в качестве базового элемента информационной безопасности угрозу уязвимости (эту угрозу создает возможность возникновения или выявления уязвимости) что позволило ввести интерпретации угрозы атаки (ее создают угрозы уязвимостей, выявление которых злоумышленником позволяет реализовать атаку) на информационную систему и угрозы безопасности информационной системы в целом соответствующими схемами резервирования (параллельного и последовательного), а также была построена математическая модель нарушителя. Эта модель основана на интерпретации сложности реализации угрозы атаки вероятностной мерой количества информации об угрозе уязвимостей, создающих угрозу атаки, которой должен обладать нарушитель для успешной атаки. Это позволило преодолеть ключевую проблему моделирования параметров и характеристик безопасности информационной системы, состоящую (при использовании иных подходов) в необходимости использования экспертных оценок как при расчете актуальности угрозы атаки [3], так и при построении модели нарушителя [4].

В настоящей работе обоснована корректность использования (и дана интерпретация получаемого при этом результата) марковских процессов при моделировании характеристик безопасности информационной системы, построены марковские модели угрозы безопасности информационной системы как системы с отказами и восстановлениями характеристик безопасности, а также с фатальным отказом, позволяющие определять важнейшие характеристики угрозы безопасности информационной системы при проектировании системы защиты информации.

Исходные данные для моделирования угрозы безопасности. Успешную атаку на информационную систему в теории информационной безопасности с существенными оговорками можно интерпретировать как отказ в теории надежности, однако задачи и методы моделирования в этих теориях принципиально различаются.

При этом необходимо отметить следующее. В отношении отдельной уязвимости (угрозы уязвимости) информационная система может рассматриваться как система с отказами и восстановлениями безопасности (угрозы систематически выявляются и устраняются), а в отношении угрозы атаки и угрозы безопасности информационной системы в целом, характеризуемой потенциальной возможностью реализации некой совокупности атак, — и как система с фатальным отказом, поскольку каждая угроза атаки с вероятностью, отличной от нуля, будет реализована нарушителем.

К угрозам уязвимостей можно отнести технологические недостатки системы, включая отсутствие требуемых функций, реализованных в системе защиты (например, возможность исполнения создаваемых пользователями файлов [5]), а также ошибки в прикладном и системном программном обеспечении, позволяющие осуществить обход реализованных функций защиты.

Можно выделить стохастические параметры угрозы уязвимости — интенсивность возникновения (выявления) λ и интенсивность устранения μ, и построить соответствующую математическую модель, позволяющую определять вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы уязвимости $P_{0\text{у}} = f(\lambda, \mu)$ [1].

В статьях [1, 2] угрозу атаки на информационную систему было предложено представлять соответствующим орграфом. При подобном представлении угроза атаки может интерпретироваться схемой параллельного резервирования уязвимостей. Угроза безопасности информационной системы также может быть представлена орграфом [1, 2]. При этом угроза безопасности может быть представлена схемой последовательного резервирования, резервируемыми и резервирующими элементами которой являются угрозы атак. Обозначим через $P_{0\text{у}m}$ вероятность того, что информационная система готова к безопасной эксплуатации в отношении m-й угрозы уязвимости, m=1, ..., M (соответствующие наборы уязвимостей создают угрозы атак), а через $P_{0\text{а}n}$ — в отношении n-й угрозы атаки, n=1, ..., N; вероятность того, что информационная система готова к безопасной эксплуатации в целом обозначим через $P_{0\text{у}}$.

Приведем пример орграфа угрозы безопасности информационной системы (система подвержена трем угрозам атак, создаваемым соответствующими угрозами уязвимостей) и проиллюстрируем принципиальные различия моделирования информационной системы в части определения характеристик безопасности и надежности (рис. 1).

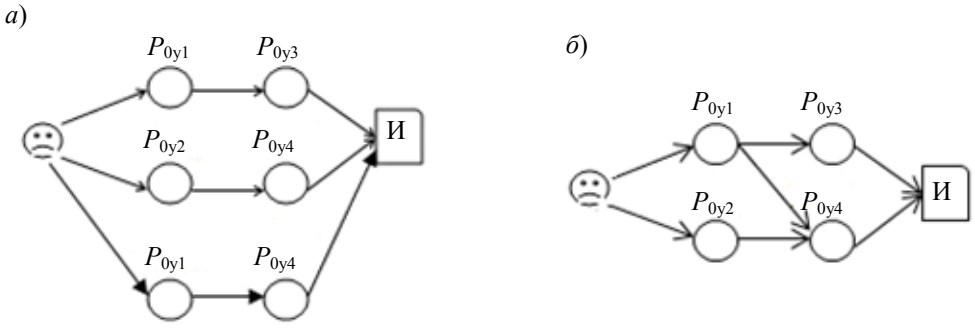

Рис. 1

На рис. 1 приведена зависимость угроз атак по угрозам уязвимостей (первая и четвертая уязвимости), позволяющая построить для исходного орграфа (*а*) приведенный орграф угрозы (*б*), в котором угроза каждой уязвимости встречается только один раз.

Замечание. Взвешенные вершины проектируемой системы защиты с параметрами $\lambda_{сз}$ и $\mu_{сз}$ включаются в соответствующие орграфы угроз атак и угрозы безопасности информационной системы [1].

Использование в качестве состояний системы в графе системы состояний угроз атак (моделирование угрозы безопасности информационной системы по угрозам атак) некорректно, поскольку некорректно предположение о том, что можно пренебречь вероятностью одномоментного появления в системе нескольких атак (марковская модель предполагает последовательное наступление в системе событий). Проиллюстрируем сказанное с помощью рис. 1. Пусть выявлены и не устранены третья и четвертая уязвимости. При выявлении при этом первой уязвимости одномоментно наступают реальные угрозы двух атак (первой и третьей). Этот вывод крайне важен, поскольку именно угроза атаки (а не угроза уязвимости) используется в качестве элемента информационной безопасности большинством известных подходов к проектированию, что не позволяет учесть зависимость угроз атак по угрозам уязвимостей и как следствие — построить корректные модели.

Таким образом, при построении марковской модели безопасности в качестве состояний системы в графе случайного процесса следует использовать угрозы уязвимостей, которые могут рассматриваться как независимые события.

Рассмотрим особенности оценивания вероятности наступления фатального отказа безопасности в информационной системе, чтобы определить, каким образом задать на марковской модели интенсивности переходов в вершину (поглощающую вершину), соответствующую фатальному отказу. Под фатальным отказом понимаем успешную атаку — осуществление несанкционированного доступа к обрабатываемой в системе информации. Сколько бы ни было одновременно создано реальных угроз атак (созданных выявленными и не устраненными уязвимостями: $P_{0an} = 0$), нарушитель в любой момент времени реализует только одну, но этого достаточно для нарушения характеристики безопасности [1]. Как следствие, вероятностью реализации в системе нарушителем одновременно двух и более атак можно пренебречь.

Исходя из того что с вероятностью $(1 - P_{0an})$, $n = 1, \ldots, N$, в системе появится n-я реальная угроза атаки, для вероятности перехода P_{an} системы из безопасного состояния S_0, в котором она находится с вероятностью $P_{0у}$, в одно из состояний фатального отказа S_n, $n = 1, \ldots, N$ (число состояний системы n+1) вследствие атаки, можем записать:

$$P_{an} = (1 - P_{0an})P_{0у}.$$

На рис. 2 приведен граф переходов цепи Маркова с фатальным отказом.

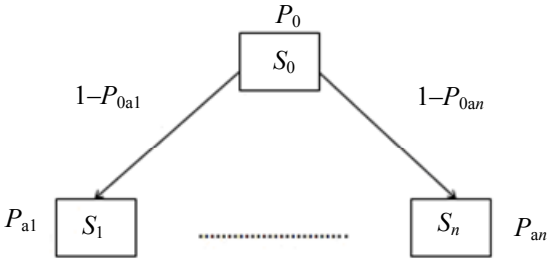

Рис. 2

С учетом того, что система находится в каком-либо состоянии:

$$P_{0у} + \sum_{n=1}^{N} P_{an} = 1$$

получим:

$$P_{0у} = 1 \Big/ \left(1 + \sum_{n=1}^{N} (1 - P_{0an}) \right).$$

Обоснование целесообразности использования марковских процессов при моделировании угрозы безопасности. В теории надежности для моделирования систем с отказами и восстановлениями объектов, как правило, используется аппарат марковских случайных процессов при допущениях о пуассоновском характере потока заявок и о показательном распределении времени обслуживания. Как известно, процесс, протекающий в физической системе, называется марковским (или процессом без последействия), если для каждого момента времени вероятность нахождения системы в будущем в любом состоянии зависит только от текущего состояния системы и не зависит от того, каким образом система пришла в это состояние.

С этой целью проанализируем, что представляют собой уязвимости, возникновение которых в системе создает реальную угрозу атаки. Уязвимость в информационной системе в общем случае может быть вызвана двумя причинами — отсутствие либо некорректность решения соответствующей задачи защиты, либо ошибки реализации средств информационной системы, например, ошибки программирования, которые могут использоваться нарушителем для обхода защиты. В качестве эксплуатационных параметров уязвимости (типа уязвимостей) будем рассматривать интенсивность возникновения уязвимости λ и интенсивность устранения уязвимости μ [1]. Под возникновением уязвимости естественно полагаем ее выявление нарушителем.

Предполагая, что система содержит конечное (пусть и очень большое) число не выявленных уязвимостей, можем заключить, что в данном случае процесс не является марковским, поскольку выявление и устранение каждой уязвимости приводит к уменьшению их числа на конечном множестве, т.е. имеет место процесс с последействием, при этом входной поток не будет являться пуассоновским, поскольку в этих предположениях $\lambda \neq \text{const}$. Однако оценим, как будут изменяться параметры уязвимости в процессе эксплуатации информационной системы. Очевидно, что в общем случае интенсивность возникновения уязвимости (типа уязвимостей) λ по прошествии некоторого времени будет снижаться, поскольку в первую очередь нарушителем будут выявляться наиболее простые недочеты в реализации защиты и ошибки в программном обеспечении (повышение сложности выявления уязвимости естественно приведет к снижению λ). Параметр μ не связан со сложностью выявления уязвимости, он определяется исключительно типом уязвимости (например, различается трудоемкость исправления ошибок в системных драйверах и в приложениях), т.е. для каждого типа уязвимости можем принять $\mu = \text{const}$.

Предположим, что спроектирована система защиты с применением формальной экстраполяции (прогнозная экстраполяция здесь малоприменима ввиду высокой интенсивности переходов на новые программные средства в современных информационных системах) и марковской модели, основанная на предположении, что $\lambda = \text{const}$ и $\mu = \text{const}$ в процессе эксплуатации информационной системы. Очевидно, что для уменьшающегося λ и $\mu = \text{const}$, используя подобную модель, можно определять граничные (при худших для системы условиях) значения требуемых характеристик.

Из сказанного можно сделать крайне важный вывод о том, что при моделировании угрозы безопасности информационной системы могут (и должны) использоваться марковские модели, которые позволяют в данном случае определять требуемые граничные значения характеристик безопасности, которые и должны применяться при проектировании систем защиты. Это существенно упрощает рассматриваемую задачу моделирования.

Марковская модель угрозы безопасности информационной системы. Рассмотрим математическое описание марковского процесса с дискретными состояниями и непрерывным временем для орграфа угрозы безопасности информационной системы, создаваемой угрозами двух атак, первая — с использованием угроз первой и второй уязвимостей, вторая — первой и третьей уязвимостей (рассматриваем зависимые угрозы атак).

Прежде всего, рассмотрим систему с отказами и восстановлениями характеристики безопасности, граф системы состояний случайного процесса для которой представлен на рис. 3 (S_0 — исходное состояние системы, S_i – в системе выявлена и не устранена одна из уязвимостей, S_{ij} — в системе выявлены и не устранены две уязвимости, S_{ijl} — в системе выявлены и не устранены все три уязвимости).

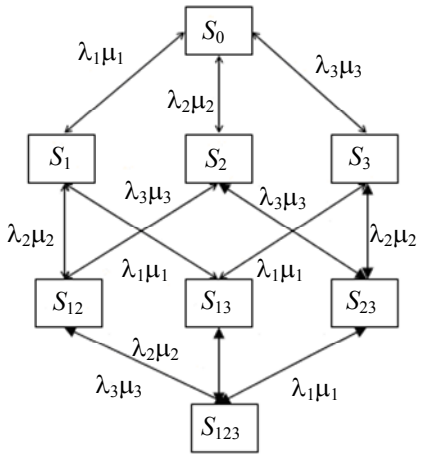

Рис. 3

Предполагаем, что все переходы системы из одного состояния в другое происходят под воздействием простейших потоков событий с соответствующими интенсивностями выявления λ_i или устранения μ_i уязвимостей, а вероятность одномоментного выявления, равно как и устранения нескольких уязвимостей, пренебрежимо мала. Переходы системы в состояния S_{12} и в S_{13} связаны с появлением в ней реальных угроз соответствующих атак. Переход из состояния S_{23} в S_{123} характеризует одномоментное возникновение в системе обеих угроз атак (при выявлении первой уязвимости в случае наличия второй и третьей), что, как видим, учитывается при этом способе моделирования. Данный граф иллюстрирует и корректность моделирования при зависимости угроз атак по уязвимостям. При подобном подходе для исходного и приведенного орграфов угрозы безопасности информационной системы получим один и тот же граф системы состояний случайного процесса, поскольку данные орграфы содержат один и тот же набор вершин и переходов между вершинами.

Используя данную модель, можно построить систему дифференциальных уравнений Колмогорова для вероятностей состояний, решив которую, можно рассчитать вероятность готовности информационной системы к безопасной эксплуатации (стационарный коэффициент готовности системы к безопасной эксплуатации).

Отметим, что при построении рассмотренной марковской модели (рис. 3) не потребовалось использование каких-либо экспертных оценок — входными параметрами модели являются стохастические параметры угроз уязвимостей, которые могут быть получены из данных статистики об их возникновении (выявлении) и устранении.

Теперь построим искомую марковскую модель системы, которая должна учитывать, что реальная угроза атаки с какой-либо вероятностью будет реализована, что приведет к фатальному отказу характеристики безопасности.

Построенная в работе [1] математическая модель нарушителя позволяет определять значение коэффициента готовности (или вероятности) к атаке на конкретную информационную систему $K_{\text{га}n}$. Основу данной математической модели составляет интерпретация сложности реализации атаки нарушителем $S_{\text{а}n}$ вероятностной мерой количества информации о потенциальной угрозе атаки, которой должен обладать нарушитель для ее реализации [1]:

$$S_{ан} = I\left(P_{0ан}\right) = -\log_2\left(1 - P_{0ан}\right).$$

Рассмотрим атаку как последовательность использования нарушителем выявленных и не устраненных в системе уязвимостей, имеющих характеристики P_{0yr} и S_{yr}, r=1, …, R, введя количественную характеристику сложности S_a ($S_a = I(P_{0a})$). Значение S_a зависит от количества информации, необходимой нарушителю для успешной атаки, угрозу которой создают R выявленных в системе и не устраненных уязвимостей

$$S_a = I\left(P_{0a}\right) = -\log_2\left(1 - P_{0a}\right) = -\log_2 \prod_{r=1}^{R}(1 - P_{0yr}),$$

где

$$P_{0a} = 1 - \prod_{r=1}^{R}(1 - P_{0yr}).$$

Используя соответствующее свойство логарифмов, можно записать:

$$S_a = I\left(P_{0a}\right) = \sum_{r=1}^{R} I\left(P_{0yr}\right) = \sum_{r=1}^{R} S_{yr}.$$

Если известны значения характеристик S_a и $S_{ан}$ (максимальная сложность реализованных, в том числе отраженных, в аналогичной информационной системе угроз атак), можно определить значение коэффициента готовности нарушителя к атаке сложности S_a:

$$K_{га} = \begin{cases} \dfrac{S_{ан}}{S_a}, \text{ если } S_{ан} < S_a, \\ 1, \text{ если } S_{ан} \geq S_a. \end{cases}$$

Замечание. При проектировании системы защиты всегда можно найти информационную систему, используемую для обработки аналогичной информации, в отношении которой протоколируются реализуемые атаки, что позволяет рассчитать значение $S_{ан}$.

Отметим, что для решения поставленной задачи не требуется задания каких-либо экспертных оценок — входные параметры могут быть получены из соответствующей непрерывно ведущейся статистики.

Имея возможность задать значение коэффициента $K_{гаn}$, можно построить искомую марковскую модель безопасности информационной системы. На рис. 4 приведен фрагмент графа состояний случайных процессов системы с фатальным отказом характеристики безопасности (рис. 3), на котором проиллюстрированы важнейшие особенности рассматриваемой модели.

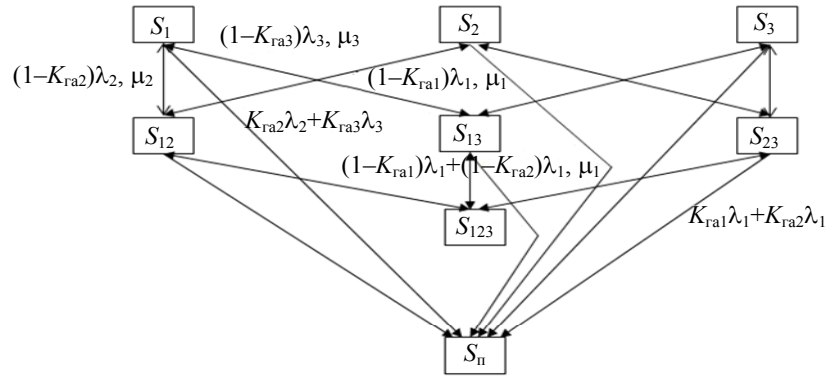

Рис. 4

На рис. 4 включено поглощающее состояние S_n, характеризующее невосстанавливаемый отказ характеристики безопасности информационной системы (атака информационной системы) — из него нет выходов.

Рассмотрим переходы между состояниями S_1 и S_n; S_{23} и S_n, обусловленные наличием в системе угроз атак, зависимых по уязвимостям. Особенность перехода из S_1 в S_n обусловливается тем, что первая уязвимость создает угрозу сразу обеих атак, следовательно, интенсивность перехода из S_1 в S_n определяется как $K_{\text{га}2}\lambda_2 + K_{\text{га}3}\lambda_3$. Особенность перехода из S_{23} в S_n обусловливается тем, что только одна атака будет реализована нарушителем. Состояние S_{23} характеризуется тем, что выявлены и не устранены вторая и третья уязвимости, как следствие, выявление первой уязвимости приводит с соответствующими вероятностями к реализации первой либо второй атаки, поэтому интенсивность перехода из S_{23} в S_n определяется как $K_{\text{га}1}\lambda_1 + K_{\text{га}2}\lambda_2$.

С целью определения искомых характеристик безопасности информационной системы для построенного таким образом графа строится система дифференциальных уравнений Колмогорова, затем — соответствующая им система линейных алгебраических уравнений, описывающих стационарный режим. Решив эту систему, можно получить вероятности искомых состояний, в том числе для поглощающей вершины, определив вероятность реализации одной из потенциальных атак на информационную систему, соответственно вероятность готовности к ее безопасной эксплуатации.

Значение вероятности P_i пребывания в определенном состоянии в марковской модели интерпретируется как среднее относительное время пребывания системы в *i*-м состоянии.

Для вычисления среднего абсолютного времени пребывания системы в каждом *i*-м состоянии T_i в системе уравнений Колмогорова нужно положить нулю все производные P_i' (P_i' =0), кроме P_0' , если считать, что в начальный момент пребывания вероятность в состоянии P_0 равна 1. Тогда, согласно теореме о дифференцировании изображений, в преобразовании Лапласа правая часть первого уравнения будет равна –1. В правых частях уравнений вместо P_i подставляются T_i, и относительно них решается система алгебраических уравнений. В результате рассчитывается среднее время наработки информационной системы до отказа (система с фатальным отказом) — до реализации на нее успешной атаки.

Эти две ключевые характеристики безопасности информационной системы могут использоваться при проектировании системы защиты.

Укрупненная марковская модель угрозы безопасности информационной системы. В марковских моделях надежности параметр потока отказов ω определяется (для стационарного участка) следующим образом:

$$\omega = \sum_{i \in Q_+} P_i \sum_{j \in Q_-} \lambda_{ij},$$

где Q_+ — множество состояний работоспособности системы, Q_- — множество состояний отказа системы, λ_{ij} — интенсивность перехода из *i*-го работоспособного состояния, вероятность нахождения системы в котором P_i, в *j*-е неработоспособное состояние.

Для построения укрупненной модели угрозы безопасности информационной системы вновь обратимся к рис. 3 и определим, как формируется поток отказов безопасности. Как видим, угроза атаки возникает в трех случаях — при переходе из состояния S_{12}, в котором система находится с вероятностью P_{12} (в марковской модели вероятность пребывания в состоянии интерпретируется как относительная доля времени нахождения системы в этом состоянии), в состояние S_{123} (это состояние реальной угрозы атаки), переходы осуществляются с интенсивностью λ_3 (с учетом соответствующей доли времени нахождения в состоянии

S_{12} — с интенсивностью $P_{12}\lambda_3$), при переходе из состояния S_{13}, в котором система находится с вероятностью P_{13}, в состояние S_{123}, переходы осуществляются с интенсивностью λ_2 (с учетом соответствующей доли времени нахождения в состоянии S_{13} — с интенсивностью $P_{13}\lambda_2$), при переходе из состояния S_{23}, в котором система находится с вероятностью P_{23} в S_{123}, переходы осуществляются с интенсивностью λ_1 (с учетом соответствующей доли времени нахождения в состоянии S_{23} — с интенсивностью $P_{23}\lambda_1$). Определяемый подобным образом поток отказов может интерпретироваться как поток возникновения реальной угрозы атаки, создаваемый в системе с интенсивностью λ_a:

$$\lambda_a = \omega = P_{12}\lambda_3 + P_{13}\lambda_2 + P_{23}\lambda_1 .$$

С учетом полученного результата может быть построена укрупненная марковская модель угрозы безопасности информационной системы в целом, создаваемой N угрозами атак, граф системы состояний случайного процесса которой представлен на рис. 5. Интенсивность перехода в поглощающее состояние $S_п$ в данном случае определяется интенсивностями возникновения реальных угроз атак $\lambda_{ап}$ и коэффициентами готовности нарушителя к реальной атаке $K_{гап}$, $n = 1, \ldots, N$.

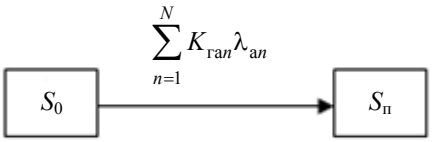

Рис. 5

Практическое использование укрупненной модели позволяет упростить задачу моделирования системы защиты, сведя ее к ряду более простых задач. При этом исходный набор угроз атак, создающих угрозу безопасности информационной системы, может быть оптимизирован (существенно сокращен) с использованием представленного в [1] метода динамического программирования, что обусловливается сильной зависимостью угроз атак по угрозам уязвимостей (многие угрозы атак создаются одними и теми же уязвимостями).

В заключение отметим, что к важнейшим результатам работы можно отнести обоснование корректности использования марковских процессов при моделировании ключевых характеристик безопасности информационной системы, выявленные и исследованные принципиальные различия постановки и решения задачи моделирования характеристик надежности и безопасности информационных систем, с учетом которых построены марковские модели угрозы безопасности информационной системы. Важным результатом проведенного исследование является обоснование необходимости рассмотрения при моделировании характеристик безопасности в качестве элемента безопасности не угрозы атаки, а угрозы уязвимости. Как показано, это обусловливается не только невозможностью в общем случае корректного задания (без учета каких-либо экспертных оценок) входных параметров модели, возможности обоснования требований к входным потокам, но и собственно невозможностью построения корректной модели, поскольку угрозы атак в общем случае являются зависимыми событиями по угрозам уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. *Щеглов К. А., Щеглов А. Ю.* Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Т. 106, № 3. С. 52—65.

2. *Щеглов К. А., Щеглов А. Ю.* Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 1(89). С. 129—139.

3. *Росенко А. П.* Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. М.: Красанд, 2010.

4. *Белов Е. Б, Лось В. П., Мещеряков Р. В., Шелупанов А. А.* Основы информационной безопасности. М.: Горячая линия—Телеком, 2006.

5. *Щеглов К. А., Щеглов А. Ю.* Защита от вредоносных программ методом контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. 2012. № 8. С. 46—51.

Сведения об авторах

Константин Андреевич Щеглов — аспирант; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 06.02.15 г.

Ссылка для цитирования: *Щеглов К. А., Щеглов А. Ю.* Марковские модели угрозы безопасности информационной системы // Изв. вузов. Приборостроение. 2015. Т. 58, № 12. С. 957—965.

MARKOV MODELS FOR INFORMATIONAL SYSTEM SECURITY THREAT

K. A. Shcheglov, A. Yu. Shcheglov

ITMO University, 197101, St. Petersburg, Russia
E-mail: info@npp-itb.spb.ru

The principal differences in formulation and solution to the problems of modeling security and reliability characteristics of information systems are studied. Applicability of the Markov models for the systems security threats based on the characteristics is analyzed. Correctness of the use of Markov processes in modeling the characteristics of information system security and reliability is justified. The necessity of consideration of the system vulnerability threat instead of an attack threat is proved. Models based on Markov processes and enlarged Markov chains for information system security, as well as a formal model of infringer are developed. The models are reported to be of possible use in development of an information system protection means.

Keywords: informational system, informational security, vulnerability threat, attack threat, informational system security threat, modeling, Markov process, Markov model, security characteristic.

Data on authors

Konstantin A. Shcheglov — Post-Graduate Student; ITMO University; Department of Computer Science, E-mail: info@npp-itb.spb.ru

Andrey Yu. Shcheglov — Dr. Sci., Professor; ITMO University; Department of Computer Science, E-mail: info@npp-itb.spb.ru

For citation: *Shcheglov K. A., Shcheglov A. Yu.* Markov models for informational system security threat // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2015. Vol. 58, N 12. P. 957—965 (in Russian).

DOI: 10.17586/0021-3454-2015-58-12-957-965