ВЕРОЯТНОСТНОЕ ПРЕДСТАВЛЕНИЕ УСЛОВИЙ СВОЕВРЕМЕННОГО РЕАГИРОВАНИЯ НА УГРОЗЫ КОМПЬЮТЕРНЫХ АТАК

Кондаков С.Е.[1], Мещерякова Т.В.[2], Скрыль С.В.[3], Стадник А.Н.[4], Суворов А.А.[5]

Аннотация. *В статье актуализируется необходимость обоснования модели нарушения безопасности инфокоммуникационной инфраструктуры (ИКИ) вследствие компьютерных атак на ее сегменты. Подобное обоснование рассматривается как предпосылка для формализации процессов реагирования на угрозы безопасности информации с целью исследования характеристик своевременности реагирования. Рассматривается ограничения на интерпретацию действий нарушителя как источника угроз безопасности информации сегментов ИКИ. Обосновывается и доказывается наличие свойств ординарности, стационарности и отсутствия последействия у потокового представления угроз компьютерных атак на сегменты ИКИ. Приводится типизация моделей нарушения безопасности информации сегментов ИКИ, классификационным основанием которой служит возможность (или ее отсутствие) комбинированного воздействия такого рода угроз. Анализируются существующие подходы к формализованному представлению характеристики эффективности действий нарушителя безопасности информации сегментов ИКИ. Формулируется общий вид условий своевременного реагирования на угрозы компьютерных атак на сегменты ИКИ, учитывающие динамику проявления угроз и реагирования на угрозы в формализованном представлении характеристик эффективности действий нарушителя. Приводится конкретизация общего вида условий своевременного реагирования на угрозы применительно к обоснованной типизации моделей нарушения безопасности информации сегментов ИКИ. Приводится общий вид аналитической модели показателя своевременности реагирования на угрозы компьютерных атак на сегменты ИКИ. Обосновываются законы распределения параметров общего вида аналитической модели для ее приведения к частному виду. Приводятся результаты вычислительного эксперимента, проводимого с целью доказательства свойств монотонности и непротиворечивости физическому смыслу показателя своевременности реагирования на угрозы компьютерных атак на сегменты ИКИ как математической функции.*

Ключевые слова: *инфокоммуникационная инфраструктура, угрозы компьютерных атак, модель нарушения безопасности информации.*

DOI: 10.21681/2311-3456-2019-6-59-68

Введение

Современная инфокоммуникационная инфраструктура (ИКИ) характеризуется наличием существенного числа сегментов, являющихся по своей природе информационными системами, предназначенными для работы с данными конфиденциального характера[6]. Функционирование этих сегментов регламентируется стандартами в сфере информационной безопасности [1-5]. Отправной точкой в исследовании проблем, связанных с обеспечением информационной безопасности[7] сегментов ИКИ, является представление модели ее нарушения как источника угроз компьютерных атак [6-8].

Ограничения на интерпретацию действий нарушителя как источника угроз компьютерных атак на сегменты инфокоммуникационной инфраструктуры

Формальная интерпретация компьютерных атак на сегменты ИКИ связана с их представлением как ре-

1 Кондаков Сергей Евгеньевич, кандидат технических наук, сотрудник Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: KCA80@yandex.ru

2 Мещерякова Татьяна Вячеславовна, кандидат физико-математических наук, начальник кафедры, Воронежский институт МВД России, г. Воронеж, Россия. E-mail: tmescherikova4@mvd.ru

3 Скрыль Сергей Васильевич, доктор технических наук, профессор, профессор МГТУ имени Н.Э. Баумана, г. Москва, Россия. E-mail: zi@bstu.ru

4 Стадник Александр Николаевич, кандидат военных наук, начальник кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: znymo@mail.ru

5 Суворов Алексей Александрович, сотрудник Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: suworow_alex@mail.ru

6 Путин В.В. Пленарное заседание Международного конгресса по кибербезопасности, 2018. URL: http://www.kremlin.ru/events/president/news/57957 (дата обращения 01.02.2019).

7 Например, Р 50.1.053–2005, ГОСТ Р 51275-2006, ГОСТ Р ИСО/МЭК 15408–1–2013, ГОСТ Р ИСО/МЭК ТО 13335-4-2007 и др.

зультата противоправных действий, совершаемых нарушителем в отношении информационных ресурсов и информационных процессов данных сегментов [9-14].

Это, в свою очередь, накладывает ограничения на интерпретацию действий нарушителя, суть которых, в общем случае, сводится к следующему:

1) нарушитель безопасности информации в ИКИ может рассматриваться в качестве как внешнего [10], так и внутреннего источника угроз компьютерных атак [14, 15];

2) за исследуемый период для такого нарушителя характерна однократность противоправных действий, связанных:

а) с получением доступа к конфиденциальной информации и ее несанкционированным копированием;

б) модификацией или уничтожением определенных массивов данных;

в) блокированием информационных процессов в сегменте ИКИ при определенных условиях.

При этом такого рода действия могут быть зависимыми [9, 16].

3) нарушение одного, двух или всех трех состояний защищенности информации в сегменте ИКИ определяется скрытностью действий нарушителя.

Указанные ограничения являются предпосылкой для представления потока угроз компьютерных атак на временном интервале $[t_1, t_2]$ исследования как потока событий, характеризующегося стационарностью, ординарностью и отсутствием последействия[8].

С целью проверки наличия свойства стационарности у рассматриваемого потока событий определим:

длительность Δt временного интервала $[t_1, t_2]$ от момента начала t_1, до момента окончания t_2 исследования угроз безопасности информации в сегменте ИКИ, $\Delta t = t_2 - t_1$;

вероятность Р(ка) компьютерной атаки на информационные ресурсы и информационные процессы сегмента;

период $T_{(ка)}$ проявления угроз компьютерных атак как длину временного интервала между двумя последовательными проявлениями такого рода угроз.

Предположение о стационарности потока угроз компьютерных атак в сегментах ИКИ базируется на выполнении двух основных условий:

его однородность во времени: вероятность Р(ка) зависит только от Δt и не зависит от его положения на временной оси, то есть для величины Р(ка) будет справедливым лишь условие: $P_{(ка)1} > P_{(ка)2}$, если $\Delta t_1 > \Delta t_2$;

моменты проявления угроз имеют одинаковую среднюю плотность λ, которая не изменяется от времени, а зависит лишь от периода проявления Т(ка):

$$\lambda = 1/T_{(ка)}. \quad (1)$$

Наличие свойства ординарности потока угроз компьютерных атак в сегментах ИКИ обусловлено однократностью противоправных действий нарушителя.

Доказательство свойства отсутствия последействия в потоке угроз компьютерных атак в сегментах ИКИ основывается на том, что угрозы появляются в последовательные моменты времени, при этом распределяясь на интервале $[t_1, t_2]$ независимо друг от друга.

Исходя из того, какие состояния защищенности информации сегмента ИКИ нарушаются, возможны три варианта модели нарушений ее безопасности, которые могут отличаться между собой возможностями (или отсутствием возможностей) нарушения одного, двух или всех трех основных состояний защищенности информации – ее конфиденциальности, целостности и доступности. В [9, 12, 14] эти варианты определены как простейшая и комбинационная модели угроз.

Термином «простейшая модель» определяется модель, для которой характерна независимость угроз компьютерных атак как предпосылки нарушения основных состояний защищенности информации сегмента ИКИ, исходя из того, что эти угрозы составляют полную группу независимых событий. Использование такой модели оправдано лишь в случае жестких ограничений на возможности нарушителя и реализации компьютерных атак в сегменте ИКИ. В исследовательском плане простейшая модель является средством оптимистической (с позиции исследователя [17]) оценки возможностей нарушителя по реализации угроз рассматриваемого типа.

Для комбинационной модели угроз компьютерных атак в сегментах ИКИ отражаются все возможные виды комбинационных воздействий на информацию с целью нарушения основных состояний ее защищенности. К возможным видам комбинационных воздействий следует отнести следующие последовательности нарушения состояний:

- нарушение целостности информации после нарушения ее конфиденциальности (комбинационная модель нарушения конфиденциальности и целостности информации);
- нарушение доступности информации после нарушения ее конфиденциальности (комбинационная модель нарушения конфиденциальности и доступности информации);
- нарушение доступности информации после нарушения ее целостности (комбинационная модель нарушения целостности и доступности информации);
- последовательное нарушение конфиденциальности, затем целостности, а затем доступности информации (комбинационная модель нарушения всех состояний защищенности информации).

В отличие от простейшей модели в рамках комбинационных моделей вероятности угроз нарушения конфиденциальности, целостности и доступности информации в сегменте ИКИ являются условными, подразумевающими выполнение одного события при условии реализации другого. Применительно к реализации нарушителем компьютерной атаки эти события связаны с выполнением следующих противоправных действий:

- несанкционированное копирование определенных массивов информации сегмента ИКИ с их последующей модификацией или уничтожением на носителе;

8 Вентцель Е.С. Исследование операций. – М.: Советское радио, 1972. – 552 с.

- несанкционированное копирование определенных массивов данных сегмента с последующим блокированием доступа к информации;
- несанкционированная модификация сегмента ИКИ или уничтожение определенных массивов данных с последующим блокированием доступа к информации;
- несанкционированное копирование определенных массивов данных сегмента ИКИ с их последующей модификацией или уничтожением на носителе, а затем блокирование доступа к информации.

Вследствие полноты отражения всех возможных действий нарушителя при реализации компьютерной атаки в сегменте ИКИ комбинационная модель является средством наиболее адекватной оценки его возможностей. Она является моделью наибольшего ущерба, наносимого информационным ресурсам и информационным процессам сегмента вследствие нарушения безопасности его информации. В исследовательском плане комбинационная модель является средством пессимистической (с позиции исследователя) оценки возможностей нарушителя по реализации угроз рассматриваемого типа.

Существующие подходы к формализованному представлению характеристики эффективности действий нарушителя по реализации угроз компьютерных атак

К настоящему времени в практике исследования угроз безопасности информации разработан ряд вариантов математического представления характеристики эффективности действий нарушителя с целью своевременной реализации угроз. Эти варианты основаны на следующих условиях [9]:

$$Э_{(ка)} = 1 \text{ при } \tau_{(р)} > \tau_{(ка)} \qquad (2)$$

и

$$Э_{(ка)} = 0 \text{ при } \tau_{(р)} \leq \tau_{(ка)}, \qquad (3)$$

где: $Э_{(ка)}$ – характеристика эффективности действий нарушителя по реализации компьютерных атак, $\tau_{(р)}$ – время реагирования на угрозу компьютерной атаки; – время реализации такого рода угрозы.

При оценке действий нарушителя условие (2) является обязательным требованием к их реализуемости. Если же условие (2) не соблюдается, то действия нарушителя теряют смысл.

Случайный характер обеих входящих в неравенство (2) величин характеризует его как случайное событие, наступающее с вероятностью $P(\tau_{(р)} > \tau_{(ка)})$. В статистическом плане данная вероятность представляет собой среднее количество ситуаций, при которых за время реализации компьютерной атаки на информационные ресурсы и информационные процессы сегмента не удавалось выполнить функции реагирования на подобного рода угрозу безопасности информации, относительно общего числа попыток ее реализации:

$$P(\tau_{(р)} > \tau_{(ка)}) = \frac{1}{I}\sum_{i=1}^{I} \alpha_i, \qquad (4)$$

где: $\alpha_i = \begin{cases} 1, \text{при } \tau_{(р)i} > \tau_{(ка)i} \\ 0, \text{в противном случае} \end{cases}$, $\tau_{(р)i}$ – время реагирования на i–ую компьютерную атаку средствами защиты информации сегмента ИКИ, $\tau_{(ка)i}$ – время реализации i–й компьютерной атаки, I – общее число компьютерных атак в течение интервала времени $[t_1, t_2]$ исследования информационных процессов в сегменте ИКИ.

С учетом того, что условия (2) и (3) составляют полную группу событий, имеет место следующее выражение для своевременности *Э(р)* реагирования на угрозы компьютерных атак:

$$Э_{(р)} = 1 - Э_{(ка)} \qquad (5)$$

Вместе с тем, исходя из (2), при обосновании характеристики *Э(ка)* эффективности действий нарушителя по реализации компьютерных атак не учитываются время начала атаки и начала реагирования на такого рода угрозу безопасности информации. Это приводит к тому, что характеристики *Э(ка)* и *Э(р)* будут корректными лишь в случае мгновенного реагирования на компьютерную атаку. Обозначив через t*(ка)* и t*(о)* – время начала компьютерной атаки и ее обнаружения средствами защиты информации, соответственно, условие мгновенного реагирования на такого рода угрозу представляется в виде:

$$t_{(о)} - t_{(ка)} \approx 0 \qquad (6)$$

Учет динамики реализации угроз компьютерных атак и реагирования на такого рода угрозы в формализованном представлении характеристик эффективности действий нарушителя

Так как на практике выполнение условия (6) является маловероятным событием, возникает необходимость обоснования вероятностного представления условий, которые учитывали бы время начала компьютерной атаки и ее обнаружения. Это, в свою очередь, предполагает разработку формальных основ математического представления характеристик эффективности действий нарушителя по реализации компьютерных атак и своевременности реагирования на такого рода угрозы для условия, альтернативного условию (6):

$$t_{(о)} - t_{(ка)} \neq 0 \qquad (7)$$

В этом случае последовательность событий, связанных с реагированием на угрозы компьютерных атак, интерпретируется математически корректно.

На примере простейшей модели нарушения безопасности информации рассмотрим условия своевременного реагирования на угрозу компьютерной атаки, учитывающие условие (7):

$$t_{(ка)} < t_{(о)}, \quad (8)$$

$$t_{(о)} < t_{(ка)} + \tau_{(ка)}, \quad (9)$$

$$t_{(о)} + \tau_{(р)} < t_{(ка)} + \tau_{(ка)} \quad (10)$$

На рис. 1 – 3 приводятся области определения условий (8) – (10), соответственно, а на рис. 4 – область выполнения этих условий.

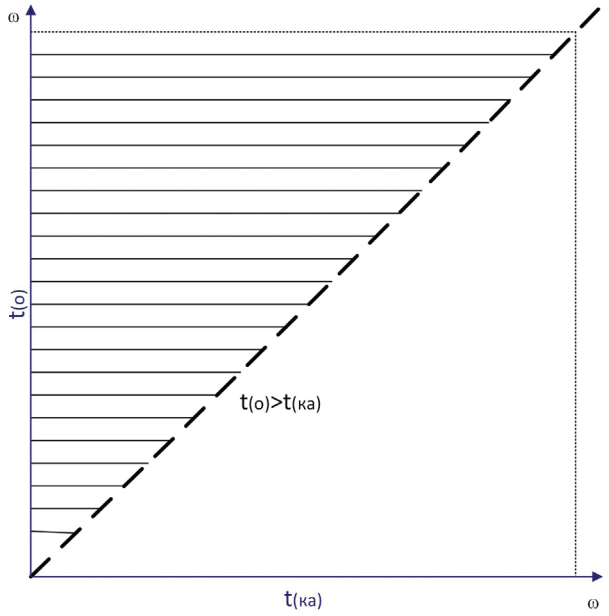

Рис.1. Графическая интерпретация области выполнения условия (8)

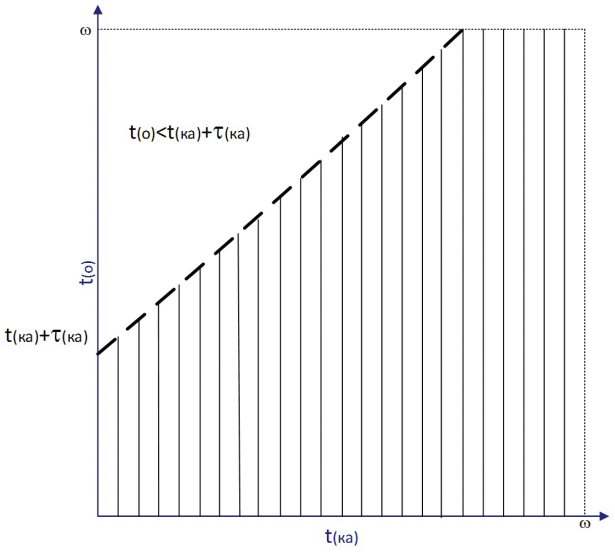

Рис. 2. Графическая интерпретация области выполнения условия (9)

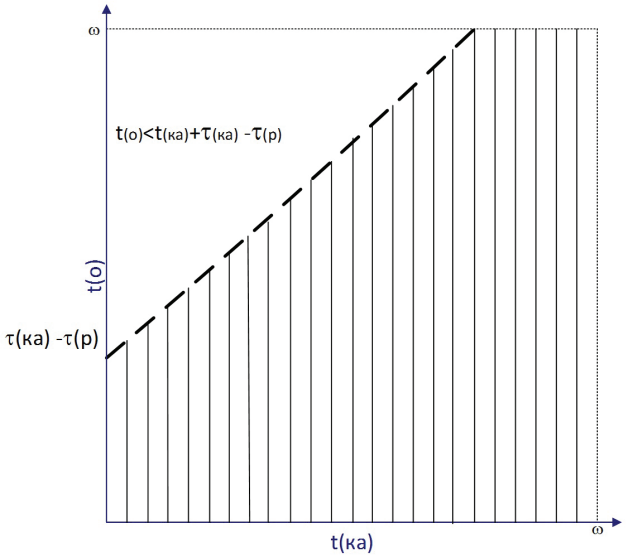

Рис. 3. Графическая интерпретация области выполнения условия (10)

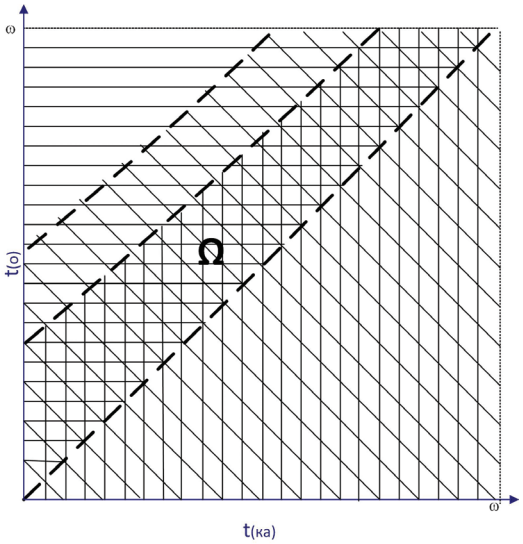

Рис. 4. Графическая интерпретация области выполнения условий (8) – (10)

Проидентифицировав индексом i цели реализации угроз компьютерных атак, условия (8) – (10) для простейшей модели можно представить в виде:

$$t_{(ка)i} < t_{(о)i}, \quad (11)$$

$$t_{(о)i} < t_{(ка)i} + \tau_{(ка)i}, \quad (12)$$

$$t_{(о)i} + \tau_{(р)i} < t_{(ка)i} + \tau_{(ка)i}. \quad (13)$$

где: i = 1 соответствует нарушению конфиденциальности информации; i = 2 соответствует нарушению целостности информации; i = 3 соответствует нарушению доступности информации.

С учетом приведенной индексации условия (8) – (10) для комбинационных моделей представляются в виде:

для случая нарушения конфиденциальности и целостности информации:

$$t_{(ка)1} < t_{(о)1} \quad (14)$$

$$t_{(о)1} < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)2} \quad (15)$$

$$t_{(о)1} + \tau_{(р)1} + \tau_{(р)2}, < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)2} \quad (16)$$

для случая нарушения конфиденциальности и доступности информации:

$$t_{(ка)1} < t_{(о)1} \quad (17)$$

$$t_{(о)1} < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)3} \quad (18)$$

$$t_{(о)1} + \tau_{(р)1} + \tau_{(р)3}, < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)3} \quad (19)$$

для случая нарушения целостности и доступности информации:

$$t_{(ка)2} < t_{(о)2} \quad (20)$$

$$t_{(о)2} < t_{(ка)2} + \tau_{(ка)2} + \tau_{(ка)3} \quad (21)$$

$$t_{(о)2} + \tau_{(р)2} + \tau_{(р)3}, < t_{(ка)2} + \tau_{(ка)2} + \tau_{(ка)3} \quad (22)$$

для случая нарушения всех состояний защищенности информации:

$$t_{(ка)1} < t_{(о)2} \quad (23)$$

$$t_{(о)1} < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)2} + \tau_{(ка)3} \quad (24)$$

$$t_{(о)2} + \tau_{(р)1} + \tau_{(р)2} + \tau_{(р)3} < < t_{(ка)1} + \tau_{(ка)1} + \tau_{(ка)2} + \tau_{(ка)3} \quad (25)$$

Случайный характер величин $t_{(о)i}$, $\tau_{(р)i}$, $t_{(ка)i}$ и $\tau_{(ка)i}$ приводит к необходимости при формировании характеристики своевременности реагирования на угрозы компьютерных атак представления условий (11) – (25) как случайных событий, характеризующихся вероятностью их выполнения. Формально эта вероятность представляет собой вероятность нахождения случайных величин $t_{(о)i}$, $\tau_{(р)i}$, $t_{(ка)i}$ и $\tau_{(ка)i}$ внутри области Ω (рис. 4).

С учетом приведенной выше номенклатуры моделей нарушения безопасности информации в сегменте ИКИ обозначим:

$\Omega_{(пм)}$ – область выполнения условий (11) – (13);

$\Omega_{(кц)}$ – область выполнения условий (14) – (16);

$\Omega_{(кд)}$ – область выполнения условий (17) – (19);

$\Omega_{(цд)}$ – область выполнения условий (20) – (22);

$\Omega_{(кцд)}$ – область выполнения условий (23) – (25).

Аналитическая модель показателя своевременности реагирования на угрозы компьютерных атак в сегментах ИКИ: представление в общем виде

С целью формального представления характеристик своевременности реагирования на угрозы компьютерных атак в сегментах ИКИ запишем выражение для вероятности нахождения случайных величин $t_{(о)}$, $\tau_{(р)}$, $t_{(ка)}$ и $\tau_{(ка)}$ внутри области Ω:

$$P(\Omega) = \int_0^{\Delta t} dx \int_0^{x+\tau_{(ка)}-\tau_{(р)}} f_1(y)\cdot f_2(x)dy - \int_0^{\Delta t} dx \int_0^{x} f_1(y)\cdot f_2(x)dy =$$

$$= \int_0^{\Delta t} f_2(x)\cdot\left[F_1(x+\tau_{(ка)}-\tau_{(р)}) - F_1(0)\right]dx - \int_0^{\Delta t} f_2(x)\cdot\left[F_1(x) - F_1(0)\right]dx = \quad (26)$$

$$= \int_0^{\Delta t} f_2(x)\cdot\left[F_1(x+\tau_{(ка)}-\tau_{(р)}) - F_1(x)\right]dx,$$

где: $f_1(y)$, $F_1(y)$, $f_2(x)$ и $F_2(x)$ – плотности и функции распределения случайных величин $t_{(о)}$ и $t_{(ка)}$ соответственно, $\Delta t = t_2 - t_1$ время, в течение которого может проявиться угроза.

Выразив $t_{(ка)}$ через $t_{(о)}$ и устремив $\Delta t \to \infty$, окончательно получим:

$$P(\Omega) = \int_0^{\Delta t} f_2(x) \cdot \left[F_1\left(x + \tau_{(ка)} - \tau_{(р)}\right) - F_1(x)\right] dx. \quad (27)$$

Исходя из рассмотренных моделей нарушения безопасности информации в сегментах ИКИ величина $t_{(ка)}$, характеризуемая плотностью распределения $f_2(x)$, может представлять собой композицию двух либо трех случайных величин.

Для комбинационных моделей нарушения конфиденциальности и целостности информации, нарушения конфиденциальности и доступности информации, а также нарушения целостности и доступности информации, плотность совместного распределения двух случайных величин описывается выражением [17]:

$$f_{(1,2)}^{(2)}(x) = \int_0^{+\infty} f_{(1)}(x) f_{(2)}(x - z) dz, \quad (28)$$

где: $f_{(1)}(x)$ – плотность распределения случайной величины $t_{(ка)1}$ для комбинационных моделей нарушения конфиденциальности и целостности информации, нарушения конфиденциальности и доступности информации и $t_{(ка)2}$ для комбинационной модели нарушения целостности и доступности информации, $f_{(2)}(x)$ – плотность распределения случайной величины $t_{(ка)3}$ для комбинационных моделей нарушения конфиденциальности и доступности информации, нарушения целостности и доступности информации и $t_{(ка)2}$ для комбинационной модели нарушения конфиденциальности и целостности информации.

Для комбинационной модели нарушения всех состояний защищенности информации плотность совместного распределения трех случайных величин описывается выражением:

$$f_{(1,2,3)}^{(3)}(x) = \int_0^{\infty} \int_0^{\infty} f_{(1)}(x) f_{(2)}(x - z) dz f_{(3)}(z - u) du dz, \quad (29)$$

где: $f_{(1)}(x)$ – плотность распределения случайной величины $t_{(ка)1}$, $f_{(2)}(x)$ – плотность распределения случайной величины $t_{(ка)2}$, $f_{(3)}(x)$ – плотность распределения случайной величины .

Частное представление аналитической модели показателя своевременности реагирования на угрозы компьютерных атак в сегментах ИКИ

Исходя из содержания параметров выражения (27) следует, что соответствующее ему аналитическое выражение может быть получено для конкретных законов распределения случайных величин: $t_{(ка)}$, $\tau_{(ка)}$ и $\tau_{(р)}$.

При обосновании законов распределения случайных величин $t_{(ка)}$ и $\tau_{(ка)}$ воспользуемся приведенными выше ограничениями на формальное представление динамики простейшей и комбинационных моделей такого рода угроз как элементарного потока событий с соответствующими свойствами стационарности, ординарности и отсутствия последействия. В учебнике Вентцель Е.С.[9] обосновано, что временной интервал между появлениями двух последовательных событий (временами $t_{(ка)}$ начала компьютерных атак) в таком потоке, а, следовательно, и часть данного интервала (время $\tau_{(ка)}$ реализации атаки) интерпретируются как случайные величины, распределенные по экспоненциальному закону.

При определении закона распределения случайных величин $\tau_{(р)}$. примем во внимание, что процесс реагирования на угрозы компьютерных атак в сегментах ИКИ составляют как минимум 12 функций [13]:

1. администрирование работы механизма защиты информации в сегменте ИКИ;
2. обеспечение санкционированного доступа;
3. разграничение доступа;
4. закрытие доступа к информации сегмента ИКИ от загрузки через внешний накопитель;
5. обеспечение целостности рабочей среды ЛВС сегмента ИКИ;
6. контроль информационных процессов в сегменте ИКИ на предмет их подверженности угрозам компьютерных атак;
7. обнаружение воздействий такого рода угроз;
8. обнаружение их источников;
9. подавление источников угроз;
10. анализ последствий компьютерных атак;
11. восстановление информации, подвергшейся атакам;
12. принятие решения о вариантах реализации информационных процессов в сегменте ИКИ в условиях компьютерных атак.

Исходя из этого случайная величина времени $\tau_{(р)}$. реагирования на угрозы компьютерных атак в сегментах ИКИ определяется как композиция времени реализации соответствующих функций, что позволяет воспользоваться положениями центральной предельной теоремы теории вероятностей (см. учебник Е.С. Венцель) и представить время $\tau_{(р)}$. как случайную величину, распределенную по нормальному (гауссову) закону распределения.

9 Вентцель Е.С. Теория вероятностей: учебник. – 11–е изд. – М.: КноРус, 2010. – 664 с.

В этом случае решением интеграла (27) является выражение:

$$P(\Omega)=\frac{1}{2}\left[e^{\frac{1}{2}\lambda(2\bar{\tau}_{(ка)}+\sigma^2\lambda-2\bar{\tau}_{(p)}-\bar{\tau}_{(o)})}\cdot\left(1-erf\left(\frac{\bar{\tau}_{(ка)}+\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)\right)+\right.$$
$$+erf\left(\frac{\bar{\tau}_{(ка)}-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)-\ e^{\frac{1}{2}\lambda(\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)})}\times$$
$$\left.\times\left(1-erf\left(\frac{\sigma^2\lambda-\bar{\tau}_{(p)}-\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)\right)+\ erf\left(\frac{\bar{\tau}_{(p)}+\bar{\tau}_{(o)}}{\sqrt{2\sigma^2}}\right)\right], \quad (30)$$

где: λ – соответствует (1), $\bar{\tau}_{(o)}$ – математическое ожидание (среднее значение) случайной величины $\bar{\tau}_{(o)}$ времени обнаружения компьютерной атаки, соответствующей длительности временного интервала $t_{(o)} - t_{(ка)}$ от времени $t_{(ка)}$ начала атаки до времени t(o) ее обнаружения, σ –среднеквадратическое отклонение случайной величины $\tau_{(o)}$.

Являясь аналитической моделью показателя своевременности реагирования на угрозы компьютерных атак в условиях различных моделей нарушения безопасности информации в сегментах ИКИ выражение (30) может использоваться как инструмент для количественной оценки эффективности используемых в сегментах средств защиты информации от несанкционированного копирования, модификации и блокирования [8, 18-20].

Вычислительный эксперимент по проверке свойств аналитической модели показателя своевременности реагирования на угрозы компьютерных атак как математической функции

С целью проверки свойств монотонности и непротиворечивости физическому смыслу аналитической модели (30), характеризующих ее как математическую функцию, проведем вычислительный эксперимент [13] по использованию данной модели для исследования процессов обеспечения доступности информации в типовом сегменте ИКИ. Для этого оценим показатель своевременности реагирования на угрозы компьютерных атак с целью блокирования информации в данном сегменте ИКИ в рамках простейшей модели нарушения безопасности информации.

Необходимые для проведения эксперимента исходные данные приведены в таблице 1 [11].

Таблица 1

.

№ п/п	Наименование параметра	Обозначение параметра	Значение параметра
1	Интенсивность компьютерных атак с целью блокирования информации в сегменте ИКИ	λ	0,000035 $с^{-1}$ (одно воздействие за восьмичасовую смену функционирования сегмента ИКИ)
2	Среднее значение случайной величины времени реализации компьютерной атаки	$\bar{\tau}_{(ка)}$	55 с
3	Среднее значение случайной величины времени обнаружения компьютерной атаки	$\bar{\tau}_{(o)}$	27,5 с
4	Среднеквадратическое отклонение случайной величины времени обнаружения атаки	σ	9,17 с
5	Среднее значение случайной величины времени реагирования на угрозу компьютерной атаки	$\bar{\tau}_{(p)}$	25 с

УДК 004.056 DOI: 10.21681/2311-3456-2019-6-59-68

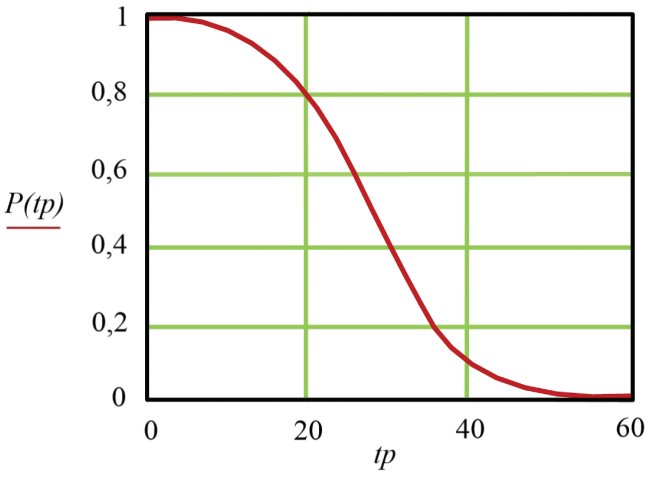

Рис. 5. Зависимость показателя своевременности реагирования на угрозы компьютерных атак с целью блокирования информации в сегменте ИКИ от времени реагирования

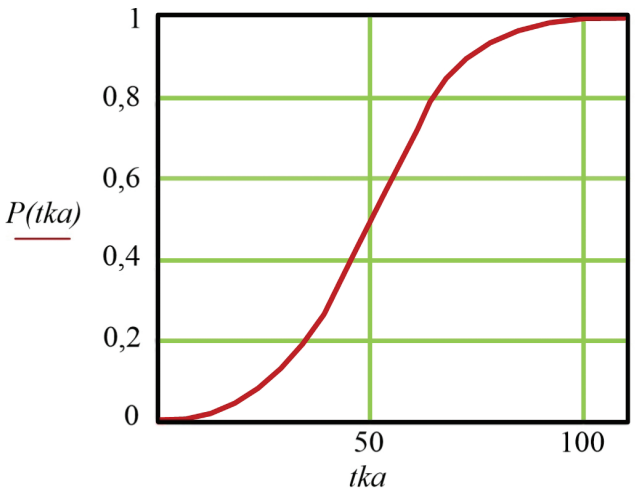

Рис. 6. Зависимость показателя своевременности реагирования на угрозы компьютерных атак с целью блокирования информации в сегменте ИКИ от времени реализации угрозы

На рис. 5 и 6 приводятся графики изменения показателя своевременности реагирования на угрозы компьютерных атак с целью блокирования информации в сегменте ИКИ при изменении параметров данного показателя. На рис. 5 в качестве изменяемого параметра рассматривается время реагирования на угрозу атаки, а на рис.6 – время ее реализации.

Как показывают результаты вычислительного эксперимента, разработанная аналитическая модель показателя своевременности реагирования угрозы компьютерных атак обладает основными свойствами математической функции – монотонностью и непротиворечивостью физическому смыслу.

Заключение

Таким образом, представленный в статье методический аппарат можно рассматривать как формальные основы синтеза вероятностных моделей условий своевременного реагирования угрозы компьютерных атак в сегментах ИКИ, что позволит существенно повысить защищенность существующих (эксплуатируемых) и перспективных (разрабатываемых) сегментов ИКИ.

Литература:

1. Арутюнов В.В. Кластеризация стандартов российской федерации в области информационной безопасности // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2017. № 5. С. 25-33.
2. Медведев Н.В., Квасов П.М., Цирлов В.Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2010. № 1 (78). С. 103-111.
3. Райкова Н.О. Сравнительный анализ стандартов менеджмента качества и информационной безопасности // Труды международного симпозиума Надежность и качество. 2014. Т. 2. С. 270-274.
4. Суханов А.В., Смирнов А.С., Хитов С.Б. Управление информационной безопасностью предприятий оборонно-промышленного комплекса в контексте стандарта ISO 27001:2013 // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2017. № 1. С. 9-16.
5. Цирлов В.Л. Правовые вопросы безопасности киберпространства в системе отечественных нормативных документов // Правовая информатика. 2014. № 2. С. 9-13.
6. Меньших В.В., Спиридонова Н.Е. Структурно-параметрическая модель несанкционированных действий нарушителя информационной безопасности // Некоторые вопросы анализа, алгебры, геометрии и математического образования. 2018. № 8. С. 216-217.
7. Чернов Д.В., Сычугов А.А. Формализация модели нарушителя информационной безопасности АСУ ТП // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 22-27.
8. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. – Воронеж: Кварта, 2018. – 588 с.
9. Мещерякова Т.В. Математические модели информационных процессов в автоматизированных информационных системах органов внутренних дел в условиях простейшей модели нарушения безопасности информации: монография / Т.В. Мещерякова, С.В. Скрыль, М.Е. Фирюлин – Воронеж: Воронежский институт МВД России, 2017. – 124 с.

10. Скрыль С.В., Киселев В.Д., Мещерякова Т.В. [и др.]. Распознавание и оценка угроз информационной безопасности территориальным сегментам единой информационно–телекоммуникационной системы органов внутренних дел: теоретические и организационно–методические основы. Воронеж: Воронежский институт МВД России, 2012. – 160 с.
11. Скрыль С.В., Рогозин Е.А., Мещерякова Т.В., Сычев А.М. [и др.]. Методы и средства повышения защищенности автоматизированных систем. Воронеж: Воронежский институт МВД России, 2013. – 108 с.
12. Скрыль С.В., Громов Ю.Ю., Сычев А.М., Мещерякова Т.В., Арутюнова В.И. Математическое представление показателя своевременности реагирования на угрозы безопасности компьютерной информации в условиях простейшей модели нарушителя. Инженерная физика. – М: «Научтехлитиздат», 2016. – №4. – С. 29 – 35.
13. Скрыль С.В., Сычев А.М., Киселев В.В., Мещерякова Т.В., Арутюнова В.И. Исследование эффективности реагирования на угрозы вирусных атак: методические основы и практика вычислительных экспериментов. Промышленные АСУ и контроллеры. – 2018. – № 6. – С. 51–62.
14. Сычев А.М., Мещерякова Т.В., Скрыль К.С., Белый Г.Ю. Формальные основы математического представления моделей нарушения безопасности информации сегментов ведомственной инфокоммуникационной инфраструктуры. Приборы и системы. Управление, контроль, диагностика. – М: «Научтехлитиздат», 2016. – №8. – С. 12 – 17.
15. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.
16. Петренко С.А., Цирлов В.Л. Импортозамещение решений IDS и SIEM // Защита информации. Инсайд. 2017. № 5 (77). С. 46-51.
17. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
18. Казарин О.В., Кондаков С.Е., Троицкий И.И. Подходы к количественной оценке защищенности ресурсов автоматизированных систем // Вопросы кибербезопасности. 2015. № 2 (10). С. 31-35.
19. Кондаков С.Е. Анализ и синтез комплекса средств защиты информации // Вопросы кибербезопасности. 2013. № 2 (2). С. 20-24.
20. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1 (1). С. 17-27.

PROBABILISTIC REPRESENTATIONS OF CONDITIONS FOR TIMELY RESPONSE TO COMPUTER ATTACK THREATS

Kondakov S.E.[10] , Meshcheryakova T.V.[11] , Skryl S.V.[12] , Stadnik A.N.[13] , Suvorov A.A.[14]

Updates are provided in the article on the need for substantiation of the model of security violations in information and communications infrastructure caused by computer attacks on its segments. Such substantiation is considered to be a prerequisite for formalizing the processes of addressing the information security threats with the aim of researching the response timeliness. Limitations related to the interpretation of intruder's actions as the source of information security threats for information and communications infrastructure segments are considered. It is explained and substantiated that flow presentation of the threats of computer attacks on information and communications infrastructure segments have the properties of ordinariness, stationarity, and absence of aftereffects. Typification is provided for the models of security violations in information and communications infrastructure segments, which is based on the probability (or absence thereof) of the combined influence of this type of threats. Existing approaches are analyzed to formalized representation of the efficiency of intruder's actions that violate the security of information and communications infrastructure segments. General type of conditions for timely response to the threats of computer attacks on information and communications infrastructure segments is formulated that take into account the dynamics of threats occurrence and response to the threats in a formalized representation of the intruder's actions efficiency parameters. The general type of conditions for timely response to threats is specified in relation to the substantiated typification of the models of security violations in information and communications infrastructure segments. General form is given for the analytical model of timeliness parameter of response to the threats of computer attacks on information and communications infrastructure segments. The laws of analytical model general form parameter distribution are substantiated to allow its reduction to the particular form. Results are described for the computational

10 Sergey Kondakov, Ph.D., Directorate of the General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: KCA80@yandex.ru
11 Tatyana Meshcheryakova, Ph.D. (Math.), Voronezh Institute of MIA of Russia, Voronezh, Russia. E-mail: tmescherikova4@mvd.ru
12 Sergey Skryl, Dr.Sc., Professor, MSTU named after N. Uh. Bauman, Moscow, Russia. E-mail: zi@bstu.ru
13 Alexander Stadnik, Ph.D.(Mil.), Krasnodar higher military school, Krasnodar, Russia. E-mail: znymo@mail.ru
14 Aleksey Suvorov, General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: suworow_alex@mail.ru

experiment performed to prove the properties of monotony and consistency with the physical meaning of timeliness parameter of response to the threats of computer attacks on information and communications infrastructure segments as a mathematical function.

Keyword: *information and communication infrastructure, cyber threats, model of a security breach information.*

References:

1. Arutyunov V.V. Klasterizaciya standartov rossijskoj federacii v oblasti informacionnoj bezopasnosti. Nauchno-tekhnicheskaya informaciya. Seriya 1: Organizaciya i metodika informacionnoj raboty. 2017. № 5. S. 25-33.
2. Medvedev N.V., Kvasov P.M., Cirlov V.L. Standarty i politika informacionnoj bezopasnosti avtomatizirovannyh sistem. Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya: Priborostroenie. 2010. № 1 (78). S. 103-111.
3. Rajkova N.O. Sravnitel'nyj analiz standartov menedzhmenta kachestva i informacionnoj bezopasnosti. Trudy mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo. 2014. T. 2. S. 270-274.
4. Suhanov A.V., Smirnov A.S., Hitov S.B. Upravlenie informacionnoj bezopasnost'yu predpriyatij oboronno-promyshlennogo kompleksa v kontekste standarta ISO 27001:2013. Nauchno-analiticheskij zhurnal Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii. 2017. № 1. S. 9-16.
5. Cirlov V.L. Pravovye voprosy bezopasnosti kiberprostranstva v sisteme otechestvennyh normativnyh dokumentov. Pravovaya informatika. 2014. № 2. S. 9-13.
6. Men'shih V.V., Spiridonova N.E. Strukturno-parametricheskaya model' nesankcionirovannyh dejstvij narushitelya informacionnoj bezopasnosti. Nekotorye voprosy analiza, algebry, geometrii i matematicheskogo obrazovaniya. 2018. № 8. S. 216-217.
7. CHernov D.V., Sychugov A.A. Formalizaciya modeli narushitelya informacionnoj bezopasnosti ASU TP. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2018. № 10. S. 22-27.
8. YAzov YU.K., Solov'ev S.V. Organizaciya zashchity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa. Monografiya. – Voronezh: Kvarta, 2018. – 588 s.
9. Meshcheryakova T.V. Matematicheskie modeli informacionnyh processov v avtomatizirovannyh informacionnyh sistemah organov vnutrennih del v usloviyah prostejshej modeli narusheniya bezopasnosti informacii: monografiya /T.V. Meshcheryakova, S.V. Skryl', M.E. Firyulin. – Voronezh: Voronezhskij institut MVD Rossii, 2017. – 124 s.
10. Skryl' S.V., Kiselev V.D., Meshcheryakova T.V. [i dr.]. Raspoznavanie i ocenka ugroz informacionnoj bezopasnosti territorial'nym segmentam edinoj informacionno–telekommunikacionnoj sistemy organov vnutrennih del: teoreticheskie i organizacionno–metodicheskie osnovy. Voronezh: Voronezhskij institut MVD Rossii, 2012. – 160 s.
11. Skryl' S.V., Rogozin E.A., Meshcheryakova T.V., Sychev A.M. [i dr.]. Metody i sredstva povysheniya zashchishchennosti avtomatizirovannyh sistem. – Voronezh: Voronezhskij institut MVD Rossii, 2013. – 108 s.
12. Skryl' S.V., Gromov YU.YU., Sychev A.M., Meshcheryakova T.V., Arutyunova V.I. Matematicheskoe predstavlenie pokazatelya svoevremennosti reagirovaniya na ugrozy bezopasnosti komp'yuternoj informacii v usloviyah prostejshej modeli narushitelya. Inzhenernaya fizika. – M: «Nauchtekhlitizdat», 2016. – №4. – S. 29 – 35.
13. Skryl' S.V., Sychev A.M., Kiselev V.V., Meshcheryakova T.V., Arutyunova V.I. Issledovanie effektivnosti reagirovaniya na ugrozy virusnyh atak: metodicheskie osnovy i praktika vychislitel'nyh eksperimentov. Promyshlennye ASU i kontrollery. – 2018. – № 6. – S. 51–62.
14. Sychev A.M., Meshcheryakova T.V., Skryl' K.S., Belyj G.YU. Formal'nye osnovy matematicheskogo predstavleniya modelej narusheniya bezopasnosti informacii segmentov vedomstvennoj infokommunikacionnoj infrastruktury. Pribory i sistemy. Upravlenie, kontrol', diagnostika. – M: «Nauchtekhlitizdat», 2016. – №8. – S. 12 – 17.
15. Skiba V.YU., Kurbatov V.A. Rukovodstvo po zashchite ot vnutrennih ugroz informacionnoj bezopasnosti. – SPb.: Piter, 2008. – 320 s.
16. Petrenko S.A., Cirlov V.L. Importozameshchenie reshenij IDS i SIEM. Zashchita informacii. Insajd. 2017. № 5 (77). S. 46-51.
17. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.
18. Kazarin O.V., Kondakov S.E., Troickij I.I. Podhody k kolichestvennoj ocenke zashchishchennosti resursov avtomatizirovannyh sistem. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. № 2 (10). S. 31-35.
19. Kondakov S.E. Analiz i sintez kompleksa sredstv zashchity informacii. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2013. № 2 (2). S. 20-24.
20. CHobanyan V.A., SHahalov I.YU. Analiz i sintez trebovanij k sistemam bezopasnosti ob»ektov kriticheskoj informacionnoj infrastruktury. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2013. № 1 (1). S. 17-27.