ИЕРАРХИЧЕСКАЯ МОДЕЛЬ ИЗМЕНЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК НА КОРПОРАТИВНУЮ СЕТЬ СВЯЗИ

М.М. Добрышин, *к.т.н., Академия ФСО России, dobrithin@ya.ru.*

УДК 004.942

Аннотация. Совершенствование средств и информационных технологий, а вместе с ними предоставляемых услуг связи, требуют расширения понятия «информационная безопасность». Принятые подходы по оценке целостности, доступности и конфиденциальности защищаемой информации недостаточно информативны при проведении оценок в информационных системах, предоставляющих своим абонентам различные услуги связи и информационного обеспечения. Для чего представлена иерархическая блочная модель, позволяющая осуществить оценку уровня информационной безопасности единичного средства обработки, хранения и передачи информации, защищенности применяемой информационной технологии, на основании которых провести оценку уровня информационной безопасности элемента сети и сети связи в целом, что и позволит оценить безопасность услуги связи. В статье представлены функциональные и аналитические взаимосвязи между изменениями значений параметров свойств защищаемых объектов в условиях различных компьютерных атак. Представление взаимосвязей в виде функциональных зависимостей является упрощенной постановкой задачи и направлением дальнейших исследований.

Ключевые слова: корпоративная сеть; компьютерные атаки; уровень информационной безопасности; иерархическая модель.

A HIERARCHICAL MODEL OF CHANGING THE LEVEL OF INFORMATION SECURITY IN THE CONTEXT OF COMPUTER ATTACKS ON THE CORPORATE COMMUNICATIONS NETWORK

M.M. Dobryshin, *Candidate of Technical Science, Academy of the FSO of Russia, employee.*

Annotation. The improvement of tools and information technologies require, and together with them, the provided communication services require the expansion of the concept of information security. The accepted approaches to assessing the integrity, accessibility and confidentiality of protected information are not informative enough when conducting assessments in information systems that provide their subscribers with various communication and information support services. For this purpose, a hierarchical block model is presented, which allows to assess the level of information security of a single means of processing, storing and transmitting information, the security of the information technology used, on the basis of which to assess the level of information security of the network element and the communication network as a whole, which will allow to assess the security of the communication service. The article presents functional and analytical relationships between changes in the values of the parameters of the properties of protected objects in the conditions of various computer attacks. The representation of relationships in the form of functional dependencies is a simplified statement of the problem and a direction for further research.

Keywords: corporate network; computer attacks; information security level; hierarchical model.

Введение

Основной полезной функцией корпоративной сети (КС) является предоставление абонентам КС услуг связи и информационного обеспечения (УС). Концепция качества обслуживания абонентов подразумевает, что услуги должны предоставляться, в том числе в условиях реализации злоумышленником различных компьютерных атак (КА).

Развитие и совершенствование средств и способов реализации КА для злоумышленника направлено на достижение цели воздействия – реализации угрозы информационной безопасности (ИБ), а для абонента и КС – на изменение в системе свойств КС, применяемых информационных технологий (ИТ), средств обработки, хранения и передачи информации (с учетом установленного комплекта программного обеспечения), а также свойств защищаемой информации [1].

Существующие подходы защиты от КА, основанные на «предположении» о цели применения КА (предполагаемые угрозы ИБ), не всегда отражают замысел деструктивных действий злоумышленника, а в некоторых случаях способствуют достижению цели воздействия.

С целью повышения обоснованности применяемых механизмов и средств обеспечения ИБ (СрОИБ) в ряде актуальных регламентирующих документах [2-5] предлагается оценивать фактическое изменение значений контролируемых параметров, на основе которых и принимать решение о формировании и реализации мероприятий по противодействию выявленной КА, например [5]:

- замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов объектов инфраструктуры;
- превышение допустимой нагрузки на вычислительные ресурсы элементов объектов инфраструктуры;
- иные нарушения в работе элементов объекта инфраструктуры, вызывающих прекращение выполнения его целевых функций.

Однако в указанных подходах оцениваются изменения значений единичных параметров (эксплуатационных характеристик), что не позволяет в полной мере оценить влияние КА на свойства защищаемого ресурса: ЭВМ, узла КС, информации, циркулирующей между узлами КС, и сеть в целом (низкая достоверность оценки), и, как следствие, снижает обоснованность реагирования на выявленный факт реализации КА (например, применение механизмов или СрОИБ, определение режимов их функционирования).

Следует также отметить, что для повышения своевременности применяемых средств и изменения режимов работы (настроек) указанных средств применяют не фактическое отклонение измеренных параметров, а прогнозные модели оценки изменения параметров, однако эти модели также обладают низкой достоверностью результатов прогнозирования влияния конкретной КА на изменение уровня ИБ КС.

Таким образом, возникает научная задача, заключающаяся в повышении достоверности результатов оценки уровня ИБ в условиях КА на элементы (узлы) КС за счет учета влияния КА на группу свойств защищаемых ресурсов.

Иерархическая модель изменения уровня информационной безопасности в условиях компьютерных атак на корпоративную сеть связи

С целью разрешения сформулированной научной задачи разработана иерархическая модель, объединяющая (рис. 1): модель изменения уровня ИБ *i*-го СОИ, вызванного КА; модель изменения уровня защищенности *k*-й ИТ, вызванного

КА; модель изменения уровня ИБ *y*-го элемента и КС, вызванного КА, и модель изменения безопасности предоставляемой *u*-й услуги связи, вызванного КА.

Выбор в качестве способа построения модели – блочный подход [6, 7], обусловлен необходимостью объединения разнородных объектов моделирования и дестабилизирующих воздействий, влияющих на эти объекты, а также структурой протекающих процессов и, в частности, тем, что безопасность предоставляемой услуги связи зависит от безопасности КС, которое, в свою очередь, определяется с организационной стороны особенностями ее построения, а с технической стороны – безопасностью применяемых СОИ и ИТ.

Модель изменения уровня ИБ *i*-го СОИ, вызванного КА, описывает изменение значений группы *j*-х параметров, характеризующих функциональные свойства *i*-го СОИ, обеспечивающих реализацию *b*-го контекста (услуги, функции) (блок 3.1, $p_a^{ibjw}(t)$) с учетом выявленных уязвимостей ИБ *i*-го СОИ $\left(\left\langle u_i^{\text{факт}}\right\rangle\right)$, в условиях влияния *a*-го вида КА с *w*-ми характеристиками на изменение значений *j*-го параметра СОИ (блок 4.1, $p_a^{ijw}(t)$), с учетом возможностей *g*-го средства обеспечения ИБ (СрОИБ) по минимизации или недопущения воздействия *a*-й КА с *w*-ми значениями параметров (блок 5.1, $z_j^{iwg}(t)$). Уровень защищенности *i*-го СОИ к *a*-й КА $\left(z_a^i(t)\right)$ и уровень защищенности *i*-го СОИ $\left(Z^{iA}(t)\right)$ к известному множеству КА (А) определяется в блоке 2.1.

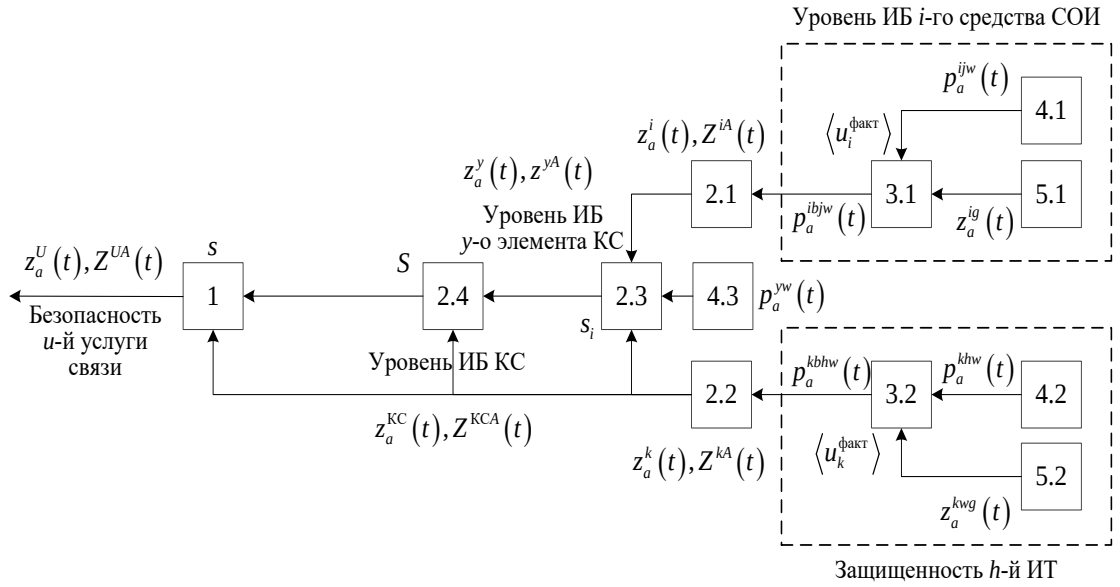

Рисунок 1

Модель изменения уровня защищенности *k*-й ИТ, вызванного КА, описывает изменение значений группы *k*-х параметров, характеризующих функциональные свойства *h*-й ИТ, обеспечивающих реализацию *b*-го контекста (услуга, функция) (блок 3.2, $p_a^{kbhw}(t)$) с учетом выявленных уязвимостей ИБ *k*-й ИТ $\left(\left\langle u_k^{\text{факт}}\right\rangle\right)$, в условиях влияния *a*-го вида КА с *w*-и характеристиками на изменение значений (блок 4.2, $P_a^{khw}(t)$), с учетом возможностей *g*-го средства обеспечения ИБ (СрОИБ) по минимизации или недопущения воздействия *a*-й КА (блок 5.2, $z_a^{kwg}(t)$

). Уровень защищенности *k*-й ИТ от *a*-й КА $\left(z_a^k(t)\right)$ и уровень защищенности *k*-й ИТ $\left(Z^{kA}(t)\right)$ к известному множеству КА (*A*) определяется в блоке 2.2.

Модель изменения уровня ИБ *y*-го элемента и КС, вызванного КА**,** описывает изменение значений параметров, характеризующих функциональные свойства *y*-го элемента (узла) КС (блок 2.3, $z^{yA}(t)$), учитывающие изменения значений параметров *i*-х СОИ $\left(Z^{iA}(t)\right)$, входящих в состав элемента, изменения значений параметров *k*-х ИТ $\left(Z^{kA}(t)\right)$, используемых в *y*-м элементе, значений *w*-го параметра, характеризующего *a*-ю КА (блок 4.3, $p_a^{yw}(t)$) на *y*-й элемент КС, а также топологию построения *y*-го элемента КС $\left(s_i\right)$. В блоке 2.4 определяется изменение уровня ИБ КС $\left(Z^{\text{KC}A}(t)\right)$ из-за КА на КС, включая изменения уровня ИБ элементов КС $\left(z^{yA}(t)\right)$, входящих в ее состав, изменение уровня защищенности применяемых для взаимодействия ИТ (блок 2.2, $Z^{kA}(t)$) и топологию КС (*S*).

Модель изменения безопасности предоставляемой *u*-й услуги связи, вызванное *КА,* описывает изменение значений параметров, характеризующих *u*-ю УС и все предоставляемые УС (*U*) (блок 1, $z_a^u(t), Z^{U\text{KA}}(t)$), вызванные КА на КС, учитывающие изменение уровня ИБ КС (блок 2.4, $Z^{\text{KC}A}(t)$), изменение уровня защищенности применяемых для взаимодействия ИТ (блок 2.2, $Z^{kA}(t)$) и топологию КС (*S*).

Исходными данными для модели являются вид (a) и значения параметров (w) КА (диапазон изменения параметров), изменение значений *j*-х или *k*-х параметров СОИ и ИТ соответственно в условиях *a*-*q* КА с *w*-*u* параметрами (значения получают на основании результатов моделирования), значения ослабляющей способности СрОИБ, топология и структура КС, схемы, описывающие взаимодействия элементов для организации и предоставления УС.

Промежуточными результатами являются изменение значений параметров, описывающих следующие свойства [8-15]:

<u>для СОИ и применяемых ИТ</u>:

– результативность – доля задач, которые выполняются правильно в условиях КА $\left(X_a^{Ri}(t)\right)$:

$$X_a^{Ri}(t) = \frac{A_a^{Ri}(t)}{B^{Ri}}, \tag{1}$$

где: $A_a^{Ri}(t)$ – количество выполненных уникальных задач при *a*-й КА на *i*-м СОИ, B^{Ri} – общее количество выполненных уникальных задач *i*-м СОИ $\left(B^{Ri} \supseteq A_a^{Ri}, A_a^R = \left(a_b^{Ria}\right), b = 1,2,...B\right)$, *t* – время реализации КА.

$$A_a^{Ri}(t) = \sum_{b=1}^{B} a_b^{Ria}(t), \tag{2}$$

$$a_b^{Ria}(t)=\begin{cases}0, \text{ если } p_a^{ibjw}(t)\geq p_a^{b\ доп}\\ 1, \text{ если } p_a^{ibjw}(t)< p_a^{b\ доп}\end{cases}, \quad (3)$$

где: $a_b^{Ria}(t)$ – b-я уникальная задача, выполняемая i-м СОИ в условиях a-й КА, $p_a^{ibjw}(t)$ – вероятность успешной реализации a-й КА с w-и характеристиками, повлекшее ухудшение значения j-го параметра, характеризующего b-ю задачу, выполняемую i-м СОИ, $p_a^{b\ доп}$ – значение вероятности реализации a-й КА, при которой b-я уникальная задача выполняется.

$$\begin{aligned}P_a^{ibjw}(t)&= f\left(P_a^{iw}(t), h_a^{ijwb}(t), \left\langle u_a^{i\ факт}\right\rangle, z_a^{ig}(t)\right)\\ P_a^{khwb}(t)&= f\left(P_a^{kw}(t), h_a^{khwb}(t), \left\langle u_a^{i\ факт}\right\rangle, z_a^{kg}(t)\right)\end{aligned}, \quad (4)$$

где: $P_a^{iw}(t)$ – функция, описывающая изменение значений w-го параметра a-й КА, $h_a^{ijwb}(t)$ – функция, описывающая изменение значений j-го параметра b-й уникальной задачи i-го СОИ или k-й параметр h-й ИТ при a-й КА с w-и характеристиками КА; $\left\langle u_a^{i\ факт}\right\rangle$ – набор выявленных уязвимостей i-м СОИ на момент начала a-й КА; $z_j^{ig}(t)$ – функция, описывающая изменение значений w-го параметра a-й КА при применении i-м СОИ g-го СрОИБ;

– эффективность / производительность – время, затраченное на успешное выполнение задачи в условиях КА $\left(X_a^{Oi}\right)$ и коэффициент затруднения работы СОИ в условиях КА $\left(x_a^{Oib}\right)$:

$$X_a^{Oi}=\frac{A_a^{Oi}}{T^{Oi}}, \quad (5)$$

где: A_{ia}^{O} – количество выполненных уникальных задач i-м СОИ при a-й КА на i-е СОИ, T^{Oi} – время на выполнение заданного количества задач i-м СОИ (задается для нормальных условий – без КА);

$$x_a^{Oib}=\frac{t_a^{Oib}}{\bar{t}^{Oi}}, \quad (6)$$

где: t_a^{Oib} – время выполнения b-й уникальной задачи при a-й КА на i-м СОИ, $\bar{t}^{Oi}$ – среднее время выполнения b-й уникальной задачи i-м СОИ в нормальных условиях – без КА.

– покрытие контекста – доля предполагаемых контекстов использования (УС и выполняемых функций), в которых СОИ или ИТ могут использоваться с приемлемым удобством использования и риском $\left(X_a^{Ki}(t), X_a^{Kk}(t)\right)$:

$$X_a^{Ki}(t)=1-\frac{\left(B^{Ki}\right)^2-\left(B^{Ki}-A_a^{Ki*}(t)\right)\left(B^{Ki}-A_a^{Ki**}(t)\right)}{\left(B^{Ki}\right)^2},$$
$$X_a^{Kk}(t)=1-\frac{\left(B^{Kk}\right)^2-\left(B^{Kk}-A_a^{Kk*}(t)\right)\left(B^{Kk}-A_a^{Kk**}(t)\right)}{\left(B^{Kk}\right)^2}, \quad (7)$$

где: $A_a^{Ki*}(t)$, $A_a^{Kk*}(t)$– количество контекстов с приемлемым удобством использования при *a*-й КА на *i*-е СОИ или *k*-ю ИТ, $A_a^{Ki**}(t)$, $A_a^{Kk**}(t)$ – количество контекстов с приемлемым риском использования при *a*-й КА на *i*-е СОИ или *k*-ю ИТ, B^{Ki}, B^{Kk} – общее количество требуемых различных контекстов использования *i*-го СОИ или *k*-й ИТ.

$$A_a^{Ki*}(t)=f\left(n_a^{ui}(t),X_a^{Oi}(t)\right)$$
$$A_a^{Kk*}(t)=f\left(n_a^{uk}(t),X_a^{Ok}(t)\right) \quad (8)$$

где: $n_a^{ui}(t)$, $n_a^{uk}(t)$ – количество операций, выполняемых для использования *u*-й УС при реализации *a*-й КА на *i*-й СОИ или *k*-й ИТ;

$$A_a^{Ki**}(t)=f\left(p_a^{ijw}(t)\right)$$
$$A_a^{Kk**}(t)=f\left(p_a^{khw}(t)\right) \quad (9)$$

где: $p_a^{ijw}(t)$, $p_a^{khw}(t)$ – вероятность реализации *a*-й КА с *w*-й характеристикой на *j*-й параметр *i*-й СОИ или *h*-й параметр, характеризующий *k*-ю ИТ.

<u>для элемента сети и сети связи (КС)</u>:

– уровень укомплектованности КС $(Y(t))$:

$$Y(t)=\frac{N^{\text{факт}}(t)}{N^0}, \quad (10)$$

где: $N^{\text{факт}}(t)$ – количество элементов КС, выполняющих функциональные задачи; N^0 – количество элементов КС в начальный момент времени;

$$N^{\text{факт}}(t)=\sum_{y=1}^{Y} n_y p_y^{\text{фз}}(t), \quad (11)$$

где: n_y – *y*-й элемент КС ($y=1,2,...Y^{\text{кс}}$ – порядковый номер элемента КС), $P_y^{\text{фз}}(t)$ – вероятность выполнения функциональных задач *y*-м элементом КС.

$$p_y^{\text{фз}}(t)=f\left(X_a^{Ri}(t),n_y^u,s_y\right), \quad (12)$$

где: n_y^u – количество УС, предоставляемых абонентам *y*-го элемента КС, s_y – топология (связность) *y*-го элемента КС;

– устойчивость (живучесть) – коэффициент оперативной готовности:

$$K^{\text{or}}(t) = f\left(k_i^{\text{or}}, Y(t), s\right), \tag{13}$$

где: k_i^{or} – коэффициент оперативной готовности *y*-го элемента КС (узла), *s* – топология (связность) элемента КС.

$$k_y^{\text{or}}(t) = f\left(X_a^{Ki}(t), s_y\right), \tag{14}$$

где: s_y – связность *y*-го элемента КС;

– пропускная способность – вероятность выполнения функциональных задач в условиях изменения пропускной способности, вызванных *a*-м КА на *y*-й элемент $\left(P_a^{\text{пс}}(t)\right)$:

$$p_a^{ywg}(t) = f\left(v_a^y(t), v^{\text{тр}\,y}(t), H_a^{yw}(t), z_a^{yg}(t)\right), \tag{15}$$

где: $v_a^y(t)$ – фактическая пропускная способность *y*-й линии (информационного потока) в условиях *a*-й КА; $v^{\text{тр}\,y}(t)$ – пропускная способность, необходимая для предоставления требуемого количества УС в заданный момент времени (*t*); $H_a^{yw}(t)$ – функция, описывающая *a*-ю КА с *w*-и параметрами на *y*-й элемент КС; $z_a^{yg}(t)$ – функция, описывающая ослабляющие способности *g*-о СрОИБ, применяемого для защиты *y*-о элемента КС;

$$v^{\text{тр}\,y}(t) \square \sum_{u=1}^{U_y} v_u^y , \tag{16}$$

где: v_u^y – требуемая скорость передачи данных для предоставления *u*-й услуги связи абонентам *y*-го элемента КС;

– вероятность выполнения функциональных задач в условиях изменения пропускной способности, вызванных *a*-м на группу элементов КА $\left(P_a^{\text{пс}}(t)\right)$:

$$P_a^{\text{пс}}(t) = f\left(v_a^{\Sigma}(t), V^{\text{КС}}(t), p_a^{yg}(t), s,\right), \tag{17}$$

где: $v_a^{\Sigma}(t)$ – фактическая пропускная способность группы линий связи (информационных потоков) в условиях *a*-й КА на КС; $V^{\text{КС}}(t)$ – пропускная способность, необходимая для предоставления требуемого количества УС в заданный момент времени (*t*); $p_a^{yg}(t)$ – функция, описывающая ослабляющие способности *g*-го механизма защиты или СрОИБ применяемого для защиты КС.

– разведзащищенность – вероятность вскрытия структуры КС $\left(P^{\text{вскр}}(t)\right)$ и идентификации информационных потоков $\left(p_y^{\text{ид}}(t), P^{\text{ид}}(t)\right)$ средствами сетевой и потоковой компьютерных разведок (КР):

$$P^{\text{вскр}}(t) = f\left(D_y^{\text{КС}}(t), s, H^{\text{СКР}}(t)\right), \tag{18}$$

где: $D_y^{\text{КС}}(t)$ – демаскирующие признаки *y*-го элемента КС, $H^{\text{СКР}}(t)$ – функция, описывающая возможности средств сетевой КР;

$$p_y^{\text{ид}}(t) = f\left(D_y^{\text{п}}(t), H_y^{\text{ПКР}}(t)\right), \tag{19}$$

где: $D_y^{\text{п}}(t)$ – демаскирующие признаки *y*-го информационного потока ($y \supseteq h$, *h*-я ИТ), $H_y^{\text{ПКР}}(t)$ – функция, описывающая возможности средств потоковой КР, выделяемых для идентификации *y*-го информационного потока КС;

$$P^{\text{ид}}(t) = f\left(p_y^{\text{ид}}(t), s, H^{\text{ПКР}}(t)\right), \tag{20}$$

где: $H^{\text{ПКР}}(t)$ – функция, описывающая возможности средств потоковой КР;

– имитостойкость – вероятность защиты от *a*-й КА, направленной на навязывание ложной информации или ложных режимов работы $\left(P_a^{\text{ис}}(t)\right)$:

$$P_a^{\text{ис}}(t) = f\left(a_{kh}^{\text{КС}}, H_a^{\text{ис}}(t)\right), \tag{21}$$

где: $a_h^{\text{КС}\,k}$ – *h*-я характеристика применяемого алгоритма идентификации (группы алгоритмов) (*k*-й ИТ), $H_a^{\text{ИС}}(t)$ – функция, описывающая *a*-ю КА, направленную на навязывание ложной информации или навязывания ложных режимов работы.

– мобильность – время (вероятность) реконфигурации КС рассматривается как механизм защиты от КА;

– криптостойкость КС не рассматривается, и предполагается, что средства криптографической защиты информации обеспечивают скрытие смыслового содержания передаваемой информации.

<u>для предоставляемых услуг связи</u>:

– действенность – вероятность установления соединения между элементами КС в условиях *j*-й КА $\left(P_a^{\text{соед}}(t)\right)$, вероятность предоставления УС в условиях КА на КС (элемент КС) $\left(P_a^{U}(t), p_a^{u}(t)\right)$, вероятность сохранения предоставляемой услуги связи в условиях КА на КС (элемент КС) $\left(P_a^{zU}(t), p_a^{zu}(t)\right)$.

<u>для восприятия услуг связи</u>:

– удовлетворенность абонентов провайдером связи – доля инцидентов ИБ, повлекших ухудшение качества предоставляемой УС, к количеству событий ИБ, зафиксированных СОИБ.

Выходными результатами моделей являются:

– для модели изменения уровня ИБ *i*-го СОИ, вызванного КА, – обобщенный показатель, характеризующий способность *i*-го СОИ выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^i(t)\right)$ и заданного множества КА (*A*) $\left(Z^{iA}(t)\right)$:

$$z_a^i(t) = 1 - \left(1 - X_a^{Ri}(t)\right)\left(1 - X_a^{Oi}(t)\right)\left(1 - X_a^{Ki}(t)\right) \tag{22}$$

$$Z^{iA}(t) = \prod_{a=1}^{A} z_a^i(t). \tag{23}$$

– для модели изменения уровня защищенности *k*-й ИТ, вызванного КА – обобщенный показатель, характеризующий способность *h*-й ИТ выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^k(t)\right)$ и заданного множества КА (*A*) $\left(Z^{kA}(t)\right)$:

$$z_a^k(t) = 1 - \left(1 - X_a^{Rk}(t)\right)\left(1 - X_a^{Kk}(t)\right) \tag{24}$$

$$Z^{kA}(t) = \prod_{a=1}^{A} z_a^k(t). \tag{25}$$

– для модели изменения уровня ИБ *y*-го элемента КС, вызванного КА:

– обобщенный показатель, характеризующий способность *y*-го элемента КС выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^y(t)\right)$ и в условиях заданного множества КА (*A*) $\left(z^{yA}(t)\right)$:

$$z_a^y(t) = 1 - \left(1 - k_a^{\text{ог}\,y}(t)\right)\left(1 - p_a^{\text{пс}\,y}(t)\right)\left(1 - p_a^{\text{ид}\,y}(t)\right)\left(1 - p_a^{\text{ис}\,y}(t)\right) \tag{26}$$

$$z^{yA}(t) = \prod_{a=1}^{A} z_y^a(t). \tag{27}$$

– обобщенный показатель, характеризующий способность КС выполнять функциональные задачи в условиях *a*-й КА $\left(z_a^{\text{КС}}(t)\right)$ и в условиях заданного множества КА (*A*) $\left(z^{yA}(t)\right)$:

$$z_{\text{а}}^{\text{КС}}(t) = 1 - \left(1 - K^{\text{ог}}(t)\right)\left(1 - P_a^{\text{пс}}(t)\right)\left(1 - P_a^{\text{вскр}}(t)\right)\left(1 - P_a^{\text{ис}}(t)\right) \tag{28}$$

$$z^{\text{КС}\,A}(t) = \prod_{a=1}^{A} z_{\text{а}}^{\text{КС}}(t). \tag{29}$$

– для модели изменения безопасности предоставляемой *u*-й услуги связи вызванного КА – обобщенный показатель, характеризующий способность КС выполнять функциональные задачи:

$$z_{\text{а}}^{U}(t) = 1 - \left(1 - P_{a}^{\text{соед}}(t)\right)\left(1 - P_{a}^{U}(t)\right)\left(1 - P_{a}^{zU}(t)\right) \tag{30}$$

$$Z^{UA}(t) = \prod_{a=1}^{A} z_{\text{а}}^{U}(t). \tag{31}$$

Заключение

Иерархическое представление рассматриваемого процесса позволило осуществить переход от оценок влияния различных видов КА на изменение свойств, характеризующих СОИ и ИТ, влияющих на качество предоставляемых услуг связи, к изменению свойств элементов КС, влияющих на качество сети.

Представленная модель (22-31) позволяет за счет комплексной оценки разнонаправленных факторов, выводящих систему из равновесного состояния, повысить достоверность оценки уровня ИБ КС и создает основу для адаптивного управления системы обеспечения ИБ, позволяющей предоставить требуемое количество услуг связи с заданным качеством в условиях различных компьютерных атак.

Сформулированные функциональные зависимости, не описанные аналитически, представляют собой постановку задачи для дальнейшего исследования.

Литература

1. Белов А. С., Добрышин М. М., Шугуров Д. Е. Функциональный подход к комплексной оценке уровня информационной безопасности элемента корпоративной сети связи // Приборы и системы. Управление, контроль, диагностика, 2023. – № 3. – С. 30-39.
2. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».
3. Приказ ФСБ России от 19.06.2019 № 282 (ред. от 07.07.2022) «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Методические рекомендации НКЦКИ по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.

5. НКЦКИ Проект. Методические рекомендации по разработке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации. 2023 г.
6. Советов Б. Я., Яковлев С. А. Моделирование систем: Учеб. для вузов – 3-е юд., перераб. и доп. – М.: Высш. шк., 2001. – 343 с: ил.
7. Добрушин М. М. Концептуальная модель оценки качества предоставления услуг связи в условиях компьютерных атак // Известия Тульского государственного университета. Технические науки, 2024. – № 2. – С. 263-269.
8. Добрышин М. М., Горбуля Д. С. Подходы оценки качества связи и предоставления услуг связи и задачи по их совершенствованию в рамках обеспечения информационной безопасности // Экономика и качество систем связи, 2023. – № 3 (29). – С. 60-71.
9. МСЭ-Т Е.802 (02/2007) Серия Е: Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы. Принципы и методики определения и применения параметров QoS.
10. Приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».
11. Давлятова М. А., Курочкина А. А., Стародубцева В. В. Оценка нормативных документов в области качества услуг, предоставляемых на базе инфотелекоммуникационной сети // Перспективы науки, 2016. – № 12 (87). – С. 107-110.
12. Квятковская И. Ю., Фам Куанг Хиеп. Система показателей оценки качества телекоммуникационных услуг и метод их оценки // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика, 2013. – № 2. – С. 98-103.
13. Давлятова М. А., Стародубцев Г. Ю., Хныкина Т. С. Эволюция развития теории и практики управления качества // Международный технико-экономический журнал, 2017. – № 2. – С. 82-85.
14. Белов А. С., Добрышин М. М., Шугуров Д. Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика, 2022. – № 11. – С. 34-40.
15. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под редакцией профессора РАН, доктора технических наук Д. П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.