Александр Л. Горбылев[1], Елена Л. Горбылева[2]
[1]*Иркутский национальный исследовательский технический университет,*
ул. Лермонтова, 83, г. Иркутск, 664074, Россия
e-mail: gal@irksecret.ru, http://orcid.org/0000-0001-8712-8055
[2]*Сибирский институт физиологии и биохимии растений*
Сибирского отделения Российской академии наук,
ул. Лермонтова, 132, г. Иркутск, а/я 317, 664033, Россия
e-mail: elnea@mail.ru, http://orcid.org/0000-0002-6858-380X

ЛИНЕЙНАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.3.06

Аннотация. Выполнен анализ и выявлены недостатки классического подхода к построению модели угроз безопасности информации, предложен способ моделирования на основе линейной системы уравнений с обратной связью. Информационная система рассматривается в данной работе как система, имеющая стационарную позицию по защищенности и объему информации, для которой обеспечивается конфиденциальность. Стационарная позиция системы зависит от коэффициентов: начальной защищенности, размеров защищаемой системы, угроз безопасности информации. Введены динамические характеристики степени безопасности информационной системы. Сформулировано условие выполнения конфиденциальности как отсутствие потока информации из информационной системы. Выполнен анализ данной линейной модели и найдена стационарная позиция системы. Получено уравнение перехода в стационарную позицию системы. На основе предлагаемой модели изучено поведение системы и переход ее в стационарное состояние при различных параметрах. Сделан вывод о том, что между защищенностью системы, угрозами безопасности информации и конфиденциальностью определенного объема информации существует взаимосвязь. Именно эта взаимосвязь приводит к стационарной позиции системы. Оценены значения параметров, при которых информация в системе теряет конфиденциальность. Предложен способ моделирования, на основании которого может быть произведена объективная оценка баланса между угрозами безопасности информации, мероприятиями по защите и объемом защищаемой информации.
Ключевые слова: динамическая модель угроз безопасности, конфиденциальность, защищенность информационной системы, динамические свойства безопасности информации.
Для цитирования: ГОРБЫЛЕВ, Александр Л.; ГОРБЫЛЕВА, Елена Л. ЛИНЕЙНАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], n. 3, p. 53-66, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1140>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.06.

Aleksandr L. Gorbylev[1], Elena L. Gorbyleva[2]
[1]*Irkutsk National Research Technical University,*
Lermontov street,83, Irkutsk,664074, Russia
e-mail: gal@irksecret.ru, http://orcid.org/0000-0001-8712-8055
[2]*Siberian Institute of Plant Physiology and Biochemistry, Siberian Division,*
Russian Academy of Sciences,
Lermontov St. 132, Irkutsk, 664033 Russia
e-mail: elnea@mail.ru, http://orcid.org/0000-0002-6858-380X

Linear dynamic model of threats to information security

DOI: http://dx.doi.org/10.26583/bit.2018.3.06

Abstract. The classic approach to the model building for information security threats is analyzed and its drawbacks are identified. A method of modeling on the base of linear equation system with a feedback was suggested. The information system was considered as a system with stationary position of security and information volume for which confidentiality is provided. Stationary position of system depends on coefficients: initial security, dimensions of protected system and threats of information security. Dynamic characteristics of information security were introduced. The condition of confidentiality as the lack of information flow from the information system is formulated. The analysis of this linear model is performed and the stationary position of the system is found. Solution of equation of transition to the system stationary position was found. On the basis of the proposed model the behavior of the system and

its transition to a stationary state under various parameters are studied. It is concluded that there is a relationship between the security system, threats to information security and the confidentiality of a certain amount of information volume. Such relationship results in system stationary position. Values of the parameters under which information in system loses confidentiality were assessed. A method of modeling on the basis of which an objective assessment of the balance between threats to information security, measures to protect and the amount of protected information can be made is proposed.
Keywords: dynamic model of security threats, confidentiality, security of information system, dynamic properties of information security.
For citation: GORBYLEV, Aleksandr L.; GORBYLEVA, Elena L. Linear dynamic model of threats to information security. IT Security (Russia), [S.l.], n. 3, p. 53-66, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1140>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.06.

Введение

В настоящее время авторами ведется разработка программного комплекса [1], который будет применяться в задаче организации адекватной защиты в ключевых системах информационной инфраструктуры (далее - КСИИ) (соответствующей нормативно-правовой базе по защите информации в ключевых инфраструктурах Российской Федерации), а также являться инструментом в защите информации в КСИИ. Одной из приоритетных задач программного комплекса является максимальная автоматизация процесса защиты информации, построения модели угроз. В данном направлении опубликованы материалы [2]. Одним из ключевых этапов в защите любой информации является этап построения модели угроз безопасности данных. В работах [3-4] рассматриваются различные подходы к классификации угроз безопасности информации и классификации уязвимостей информационной системы. Одним из результатов работ является вывод о том, что количество уязвимостей в системе невозможно зафиксировать на данный момент.

Рассмотрим классический подход построения модели угроз безопасности информации как в ключевых системах информационных инфраструктур, так и в других информационных системах, например, в информационной системе персональных данных [5] и как пример реализации [6], отображенный на рис. 1.

Рис. 1. Принципиальная схема определения актуальных угроз безопасности
(Fig. 1. The basic scheme of determining the actual security threats)

В классическом (статическом) подходе эксперт в области безопасности информации обладает следующей информацией об угрозе безопасности информации:

$$T_i = [S_j, V_n, M_m, O_k], \quad (1)$$

где T_i– множество угроз, S_j– множество источников угроз, V_n– множество уязвимостей информационной системы, M_m– множество способов реализации угрозы, O_k– множество объектов воздействия.

Далее подход сводится к использованию методики определения актуальности угроз безопасности информации. Как правило, методика заключается в построении матрицы, элементами которой являются вербальные интерпретации опасности угрозы, ее вероятного появления и элементы таблицы истинности, возможен вариант с масштабом системы. В зависимости от заданной таблицы истинности делается вывод об актуальности угрозы. Например, методика определения актуальных угроз безопасности информации персональных данных [7] табл. 1.

Таблица 1. Вербальная интерпретация методики определения актуальных угроз безопасности информации

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	**Высокая**
Низкая	неактуальная	неактуальная	**актуальная**
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Приведение угрозы для конкретной системы к одному из уровней реализации угрозы не является на данный момент объективным методологически. Приведение угрозы к определенной степени опасности не подкреплено объективными данными, такими как статистический анализ. Операция выбора опасности угрозы и операция выбора возможности реализации угрозы выполняются на основе опыта эксперта, использующего методику, что является несомненным пробелом в данном мероприятии. Статья [8] вводит понятие процесса в построение модели угроз и опирается на информационные потоки, что уже подводит нас к понятию динамики. Также работа [9] раскрывает временные рамки атак типа stuxnet. Известны более развернутые подходы [10], в которых вводятся состояния системы, переходы из одного состояния в другое. Остается важным вопрос об объективной оценке эффективности средств защиты информации [11]. В статье рассматривается методика определения эффективности обеспечения данных от угроз нарушения целостности. В работах [12-13] авторы выполнили анализ автоматизированных средств анализа защищенности система. В статье [14] авторы делают акцент на выявлении элементов информационной системы на аппаратном, программных уровнях и связей между ними. Рассмотрим динамическое моделирование на примере работы автора данной статьи [15] из другой предметной области. Математическим результатом работы является динамическое уравнение. Приближая вплотную в динамике, с введением фактора времени, авторы работы [16], рассматривают по временной шкале угрозы, исходящие от инсайдера. Из практики известен пример [17] рассмотрения информационной системы и ее защиты от угроз безопасности информации в режиме реального времени. Несомненно, рассматриваются динамические модели в работах [18-20]. Хорошо иллюстрирует динамический подход модель реакции системы на угрозу.

Обратная связь характеристик безопасности информации

Рассмотрим характеристики безопасности информации или свойства информации, такие как конфиденциальность, доступность, целостность. Будем понимать под конфиденциальностью информации свойство информации быть доступной определенному кругу лиц. Нарушение конфиденциальности – информация стала доступной неопределенному кругу лиц. Доступность информации – свойство информации быть полученной за приемлемый промежуток времени. Нарушение доступности – невозможность получить информацию за приемлемый промежуток времени. Целостность информации – свойство информации не быть измененной

несанкционированно. Нарушение целостности – несанкционированное изменение информации. Проклассифицируем данные свойства по критерию обратной связи (рассматриваем системно) и критерию возврата к первоначальному состоянию. По критерию обратной связи – при нарушении целостности и доступности мы можем гарантированно зафиксировать данный факт. При нарушении конфиденциальности гарантированно зафиксировать данный факт невозможно. При нарушении доступности и целостности данные характеристики возможно восстановить. При нарушении конфиденциальности восстановить ее невозможно, обобщение отображено в табл. 2.

Таблица 2. Классификация множеств свойств информации

№ п/п	Свойство информации	Критерий «обратной связи»	Критерий восстановления исходного состояния
1	Конфиденциальность	-	-
2	Доступность	+	+
3	Целостность	+	+

К вышеизложенному можно добавить, что конфиденциальность - понятие «ортогональное» к целостности и доступности, но доступность не является «ортогональной» к целостности. Таким образом, имеет смысл рассматривать свойства безопасности информации в виде двух множеств C, IA, где множество $C = \{c\}$, множество элементов «конфиденциальности» с мощностью 1. $IA = \{i, a\}$, множество элементов «целостнодоступного» множества с мощностью множества в 2 элемента.

Динамическая модель угроз безопасности информации. **Динамическая конфиденциальность**

Рассматривая методику определения угроз безопасности, как и сами угрозы, можно заметить, что описание сводится к наличию свойств и выбору по критериям. Эксперту необходимо просто переписать угрозу из одной таблицы в другую. В данном подходе нет временных параметров угроз безопасности информации, временных параметров цикла существования информационной системы и даже временных параметров свойств информации явно. Введем некоторые из них. Известно, что конфиденциальность - это свойство информации быть доступной определенному кругу лиц, что выражено качественно. Как сделать вывод, что система скомпрометирована и информация потеряла свойство конфиденциальности? Логично предположить, что информация должна стать известной лицам, не входящим в определенный перечнем список лиц. Потеря такого качества, как конфиденциальность – процесс, имеющий временной интервал. Обозначим количество информации в системе - I. Поток информации за пределы информационной системы - dI, скорость изменения этого потока $-\frac{dI}{dt}$. Логично, что если поток и скорость изменения потока равны нулю, то утечки информации нет:

$$dI = 0; \frac{dI}{dt} = 0 \ . \tag{2}$$

От чего может зависеть утечка информации? Прежде всего от защищенности системы - принятых мер на нейтрализацию угроз безопасности информации. D– показатель защищенности информационной системы. Составим уравнение:

$$\frac{dI}{dt} = C_{d1} * D - C_v * I, \tag{3}$$

где C_v - коэффициент, отображающий влияния количества информации на ее утечку; C_{d1} - коэффициент, отображающий влияние защищенности на утечку информации.

Интерпретировать данное уравнение можно следующим образом. Утечка информации зависит:

- от размера информационной системы (следовательно, в какой-то мере и от количества информации);
- утечка информации купируется защищенностью системы (мерами по нейтрализации угроз безопасности информации).

Далее рассмотрим, от чего зависит защищенность системы - D. Определим защищенность системы как способность системы противостоять несанкционированному доступу к конфиденциальной информации. Следовательно, защищенность системы будет зависеть:

- от размеров системы (как и от количества информации);
- угроз безопасности информации.

Составим уравнение:

$$\frac{dD}{dt} = D_p - C_{d2} * I - V_d * I, \tag{4}$$

где D_p – коэффициент, отображающий влияние мероприятий по защите информации; C_{d2} – коэффициент, отображающий влияние размеров системы на защищенность. V_d – коэффициент, отображающий влияние угроз безопасности информации на защищенность информационной системы. Объединим уравнение (3) и (4) в систему.

$$\begin{cases} \frac{dI}{dt} = C_{d1} * D - C_v * I \\ \frac{dD}{dt} = D_p - C_{d2} * I - V_d * I \end{cases} \tag{5}$$

Найдем стационарную позицию системы, описываемую уравнениями (5). Условия стационарности $dI = 0; \frac{dI}{dt} = 0$.Следовательно:

$$\begin{cases} C_{d1} * \bar{D} - C_v * \bar{I} = 0 \\ D_p - C_{d2} * \bar{I} - V_d * I = 0 \end{cases} \tag{6}$$

Из второго уравнения системы следует:

$$\bar{I} = \frac{D_p}{C_{d2} + V_d} \tag{7}$$

Далее из первого уравнения системы уравнений (6) находим $\bar{D}$.

$$C_{d1} * \bar{D} - \frac{C_v * D_p}{C_{d2} + V_d} = 0 \tag{8}$$

$$\bar{D} = \frac{C_v * D_p}{C_{d2} + V_d} * \frac{1}{C_{d1}} \tag{9}$$

Следовательно, условия позиции стационарности системы:

$$\begin{cases} \bar{I} = \dfrac{D_p}{C_{d2} + V_d} \\ \bar{D} = \dfrac{C_v * D_p}{C_{d2} + V} * \dfrac{1}{C_{d1}} \end{cases} \quad (10)$$

Решим систему уравнений (5) методом «малых отклонений»:
$I = \bar{I} + I; D = \bar{D} + D$, следовательно, система уравнений примет вид:

$$\begin{cases} \dfrac{dI}{dt} = C_{d1} * (\bar{D} + D) - C_v * (\bar{I} + I) \\ \dfrac{dD}{dt} = D_p - C_{d2}(\bar{I} + I) - V_d(\bar{I} + I) \end{cases} \quad (11)$$

$$\begin{cases} \dfrac{dI}{dt} = C_{d1} * (\dfrac{C_v * D_p}{C_{d2} + V_d} * \dfrac{1}{C_{d1}} + D) - C_v * (\dfrac{D_p}{C_{d2} + V_d} + I) \\ \dfrac{dD}{dt} = D_p - C_{d2} * (\dfrac{D_p}{C_{d2} + V_d} + I) - V_d * (\dfrac{D_p}{C_{d2} + V_d} + I) \end{cases} \quad (12)$$

$$\begin{cases} \dfrac{dI}{dt} = \dfrac{C_{d1} * C_v * D_p}{C_{d2} + V_d} * \dfrac{1}{C_{d1}} + C_{d1} * D - \dfrac{C_v * D_p}{C_{d2} + V_d} - C_v * I \\ \dfrac{dD}{dt} = D_p - \dfrac{C_{d2} * D_p}{C_{d2} + V_d} - C_{d2} * I - \dfrac{V_d * D_p}{C_{d2} + V_d} - V_d * I \end{cases} \quad (13)$$

$$\begin{cases} \dfrac{dI}{dt} = C_{d1} * D - C_v * I \\ \dfrac{dD}{dt} = -I(C_{d2} + V_d) \end{cases} \quad (14)$$

Дифференцируем первое уравнение системы (14) и получаем:

$$\frac{d^2 I}{dt^2} = -I * C_{d1} * (C_{d2} + V_d) - C_v * \frac{dI}{dt} \quad (15)$$

$$\frac{d^2 I}{dt^2} + C_v * \frac{dI}{dt} + I * C_{d1} * (C_{d2} + V_d) * I = 0 \quad (16)$$

Уравнение (16) является уравнением гармонического осциллятора с затухающей амплитудой, где

$$\omega_0 = \sqrt{C_{d1} * (C_{d2} + V_d)} \quad (17)$$

$$\omega = \sqrt{C_{d1} * (C_{d2} + V_d) - \frac{C^2_v}{4}} \quad (18)$$

$$T = \frac{2 * \pi}{\sqrt{C_{d1} * (C_{d2} + V_d) - \dfrac{C_v^{\,2}}{4}}} \quad (19)$$

$$\beta = \frac{C_v}{2} \quad (20)$$

Решение уравнения гармонического осциллятора распадается на три случая.

1. $\beta < \omega_0$:

$$I = A_0 * \exp(-\frac{C_v}{2}) * \cos(\sqrt{C_{d1} * (C_{d2} + V_d) - \frac{C^2_v}{4}} * t + \varphi_0), \quad (21)$$

где A_0 – константа (первоначальная амплитуда), φ_0- первоначальная фаза.

2. $\beta = \omega_0$:

$$I = (A_0 + B_0 * t) * \exp(-\frac{C_v}{2} * t), \quad (22)$$

где A_0 – константа (первоначальная амплитуда).

3. $\beta > \omega_0$:

$$I = A_0 * \exp(-\gamma_1 * t) + B_0 * \exp(-\gamma_2 * t), \quad (23)$$

где $\gamma_{12} = \beta \pm \sqrt{\frac{C^2_v}{4} - C_{d1} * (C_{d2} + V_d)}$

Рассмотрев три варианта решения уравнения около стационарного положения системы, можно прийти к выводу, что, исходя из условий соотношения диссипации и собственной частоты колебаний величины I, затухание последней к определенному значению осуществляется периодически, с затухающей амплитудой, или по экспоненциально затухающему закону.

Выполним более наглядный анализ поведения системы, перейдя от дифференциальной формы уравнений (5, 6) к дискретной и промоделировав некоторый интервал существования системы. А именно:

$$\begin{cases} \frac{I_{n+1} - I_n}{\Delta t} = C_{d1} * D_n - C_v * I_n \\ \frac{D_{n+1} - D_n}{\Delta t} = D_p - C_{d2} * I_n - V_d * I_n \end{cases} \quad (24)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1} * D_n - C_v * I_n) * \Delta t \\ D_{n+1} = D_n + (D_p - I_n * (C_{d2} + V_d)) * \Delta t \end{cases} \quad (25)$$

Первоначально примем коэффициенты C_{d1}, C_v, C_{d2}, D_p за единицу. Следуя из условия стационарной позиции системы, I и D будут равны 0.5 и 0.5. Шаг моделирования примем за 0.1 для всех итераций моделирования, поэтому в таблице отображать его не будем. Величины I_{sp}, D_{sp} отображают стационарные значения параметров, если таковые были достигнуты за конечное число итераций. Количество итераций было принято равным 1000. Далее проведем имитационное моделирование для значений $\beta < \omega_0, \beta \quad \omega_0, \beta > \omega_0$, с отклонением от стационарной позиции системы. Данные представим в табл. 3.

Таблица 3. Параметры моделирования и их вербальная интерпретация

№ п/п	I	D	C_v	C_{d1}	D_p	C_{d2}	V_d	I_{sp}, D_{sp}	Параметры
1	0,5	0,5	1	1	1	1	1	0.5, 0.5	стац. позиция
2	0,5	0,5	0,5	1	1	1	1	0.5, 0.25	$\beta < \omega_0$
3	0,5	0,5	2,82	1	1	1	1	0.5, 1.41	$\beta \quad \omega_0$
4	0,5	0,5	4	1	1	1	1	0.5, 2	$\beta < \omega_0$

5	0,5	0,5	1	1	1	1	5	0.16, 0.16	$\beta \quad \omega_0$
6	0,5	0,5	10	1	1	1	1	0.5, 5	$\beta \quad \omega_0$
7	0,5	0,5	1	1	10	1	1	5,5	$D_p \quad 1$
8	10	10	1	1	1	1	1	0.5, 0.5	$I_0 \neq I_{sp}, D_0 \neq D_{sp}$
9	10	1	1	1	1	1	1	0.5, 0.5	$I_0 \neq I_{sp}, D_0 \neq D_{sp}$ $I_0 \neq D_0$
10	1	10	1	1	1	1	1	0.5, 0.5	$I_0 \neq I_{sp}, D_0 \neq D_{sp}$ $I_0 \neq D_0$

Визуализация результатов.

Далее на рисунках 2-11 отображено поведение величин I, D по прохождению итераций. Параметры: $I, D, C_v, C_{d1}, D_p, C_{d2}, V_d$ подставлены согласно табл. 2.

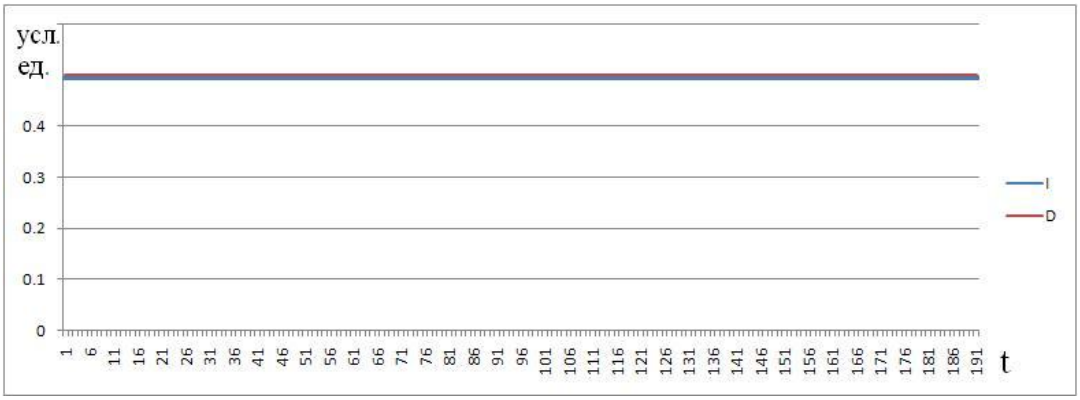

Рис. 2. Отображение стационарной позиции по количеству итераций
(Fig. 2. Displaying a stationary position by the number of iterations)

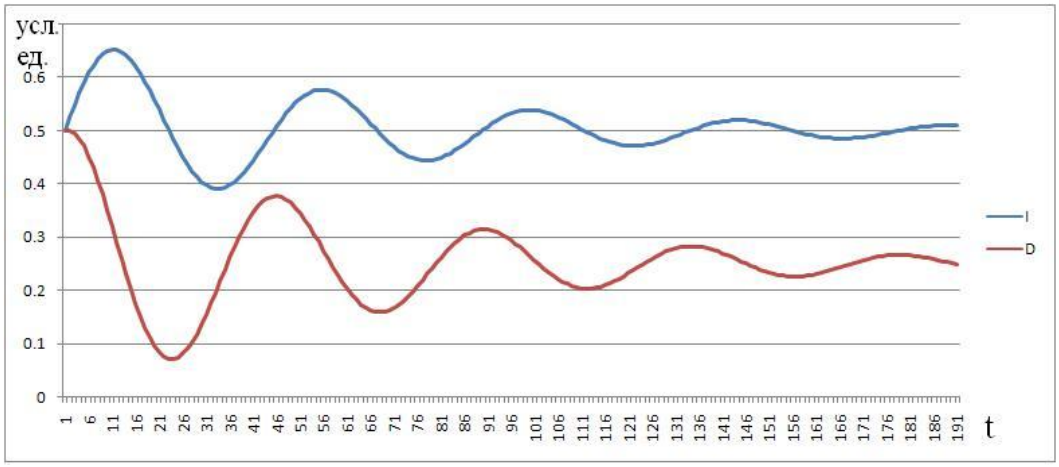

Рис. 3. Условие $\beta < \omega_0$
(Fig. 3. Condition $\beta < \omega_0$*)*

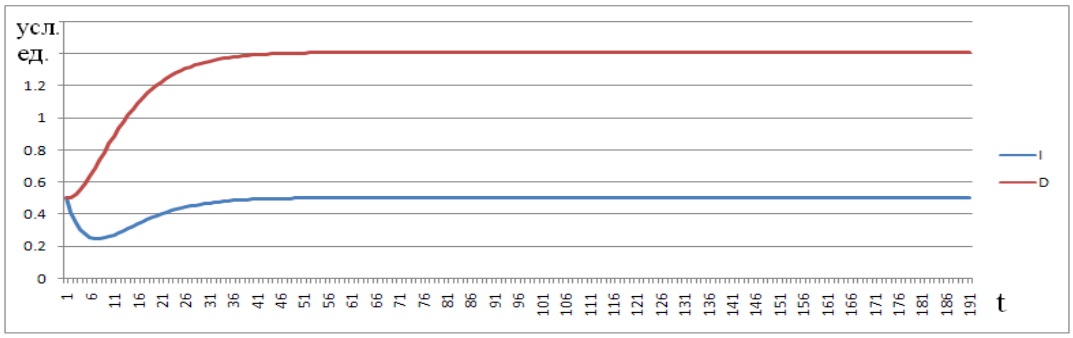

Рис. 4. Условие $\beta \quad \omega_0$

(Fig. 4. Condition $\beta \quad \omega_0$)

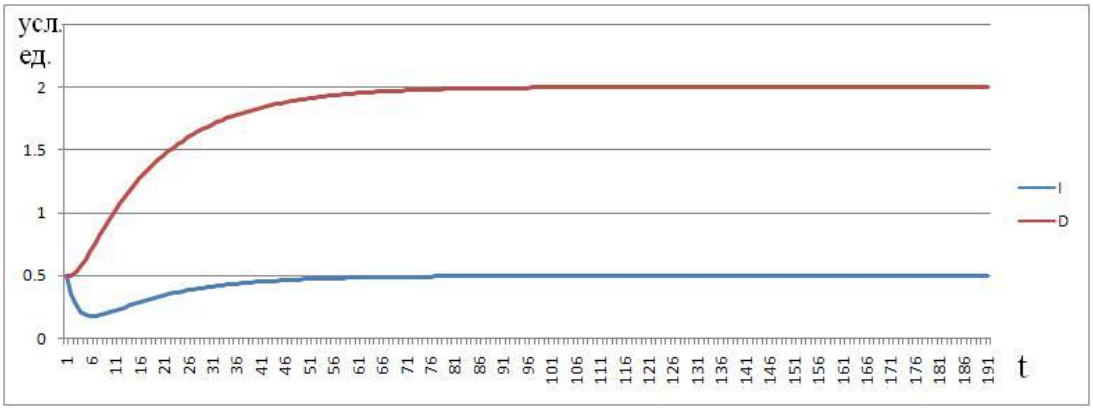

Рис. 5. Условие $\beta > \omega_0$

(Fig. 5. Condition $\beta > \omega_0$)

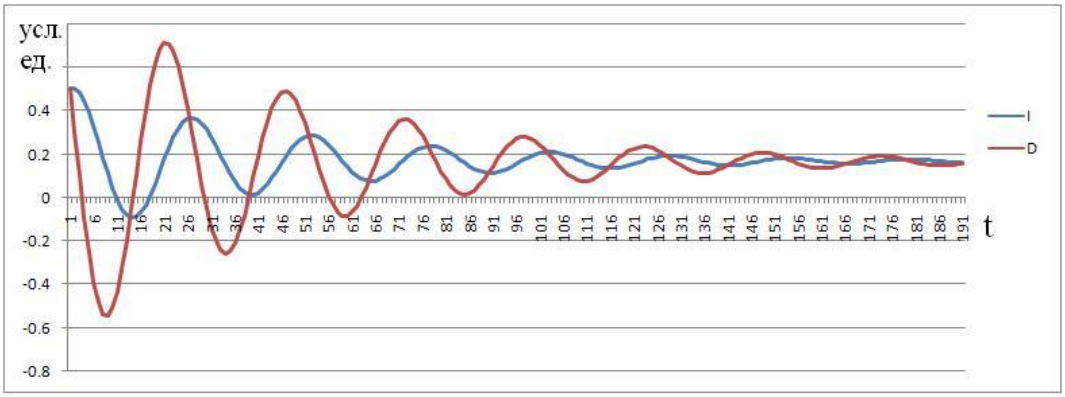

Рис. 6. Условие $\beta \quad \omega_0$

(Fig. 6. Condition $\beta \quad \omega_0$)

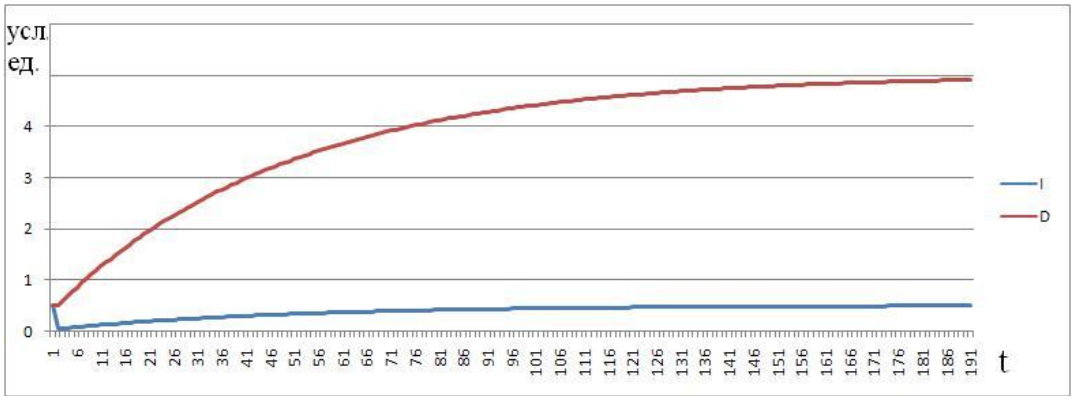

Рис. 7. Условие $\beta \quad \omega_0$

(Fig. 7. Condition β ω_0)

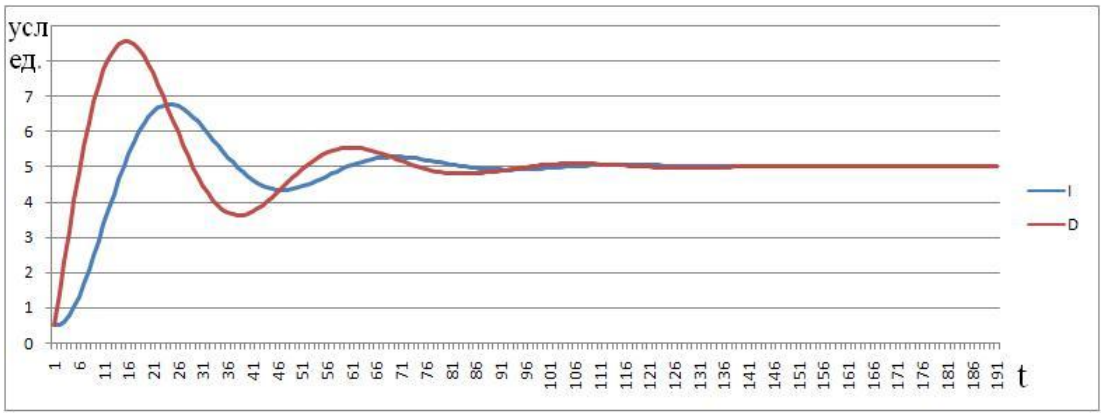

Рис. 8. Условие D_p 1

(Fig. 8. Condition D_p 1)

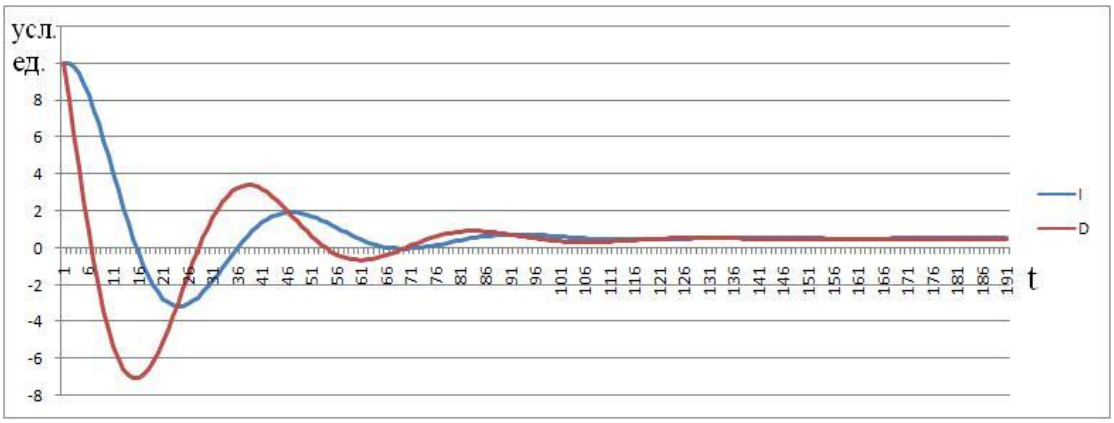

Рис. 9. Условие $I_0 \neq I_{sp}, D_0 \neq D_{sp}$

(Fig. 9. Condition $I_0 \neq I_{sp}, D_0 \neq D_{sp}$)

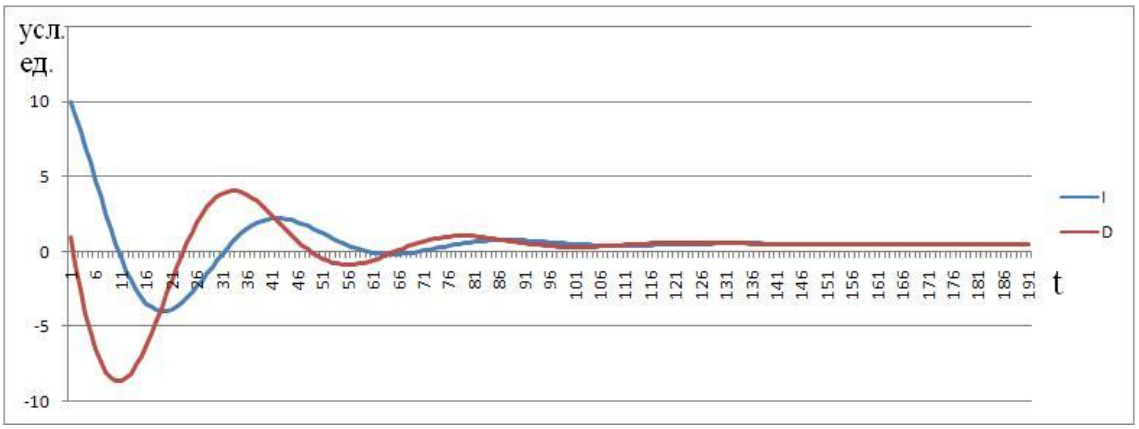

Рис. 10. Условие $I_0 \neq I_{sp}, D_0 \neq D_{sp}, I_0 \neq D_0$

(Fig. 10. Condition $I_0 \neq I_{sp}, D_0 \neq D_{sp}, I_0 \neq D_0$)

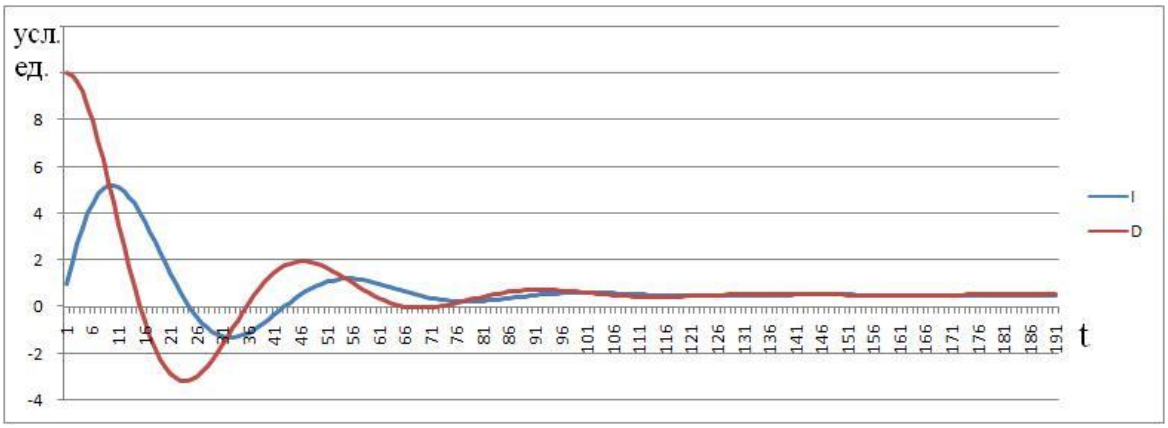

Рис. 11. Условие $I_0 \neq I_{sp}, D_0 \neq D_{sp}, I_0 \neq D_0$

(Fig. 11. Condition $I_0 \neq I_{sp}, D_0 \neq D_{sp}, I_0 \neq D_0$*)*

Интерпретация полученных графических результатов

Рис. 2 показывает стационарную позицию системы, что аналитически подтверждается системой равенств (10). Графическое отображение поведения системы для $\beta < \omega_0$зафиксировано на рис. 3. Заметны периодические затухающе колебания. При этом стационарные значения величин D(защищенность) и I(количество информации) отличаются друг от друга. Видно, что меньшей мерой защищенности системы обеспечивается тот же уровень количества информации, что и в случае с $C_v = 1$, так как обратная отрицательная связь влияния объема информации меньше $C_v = 0.5$. Рис.4 и 5 демонстрируют не колебательный процесс, что подтверждается аналитически. При данных значениях β, ω_0система быстро переходит в стационарное состояние, что логично, поскольку отрицательная обратная связь стала сильнее. Рис. 6 демонстрирует поведение системы с преобладанием обратной отрицательной связи за счет большого коэффициента угроз безопасности информации. Данный факт вносит в стационарное состояние величин защищенности и количества информации уменьшение значения последних. Такой переход «губителен» для системы, несмотря на то, что система вернется в стационарную позицию, из-за большой амплитуды конфиденциальность «растеривается» по пути к этой стационарной позиции. Рис.7 иллюстрирует большую отрицательную связь от размеров системы, что и было зафиксировано на рис. 3 и 4. При этом показатель защищенности системы возрастает многократно, чтобы быть в «балансе» со значением $I = 0.5$. Рис. 8 демонстрирует колебательное вхождение в стационарное состояние, при котором количество информации и защищенность системы многократно увеличились за счет коэффициента «мероприятий по защите информации». Рис. 8-10 обобщает тот факт, что независимо от первоначальных значений защищенности и количества информации, последние сходятся к одним и тем же значениям. Подтверждается факт о том, что от первоначальных значений стационарные значения величин I, Dне зависят. На основе анализа можно утверждать, что количество защищаемой информации (как и масштаб системы) связано с показателем защищенности системы, угрозами и внутренними механизмами системы, и это соответствие имеет стационарную позицию.

Дальнейшие исследования и практическая значимость

Принимая во внимание полученные результаты работы, можно сделать вывод о необходимости дальнейшего исследования динамических уравнений с характеристиками целостности и доступности информации. Несомненно, учитывается, что модель в данной работе абстрактная, простая и требует дальнейшего развития с целью конкретизации, применения к реальным системам. Практическая значимость заключается в динамическом подходе, который дает ответ на вопрос о балансе применяемых мер защиты информации и

масштабе информационной системы. Сформулирована отправная точка для приведения измерения эффективности мероприятий по защите информации и приведения мероприятий по защите информации к единому знаменателю.

Заключение

Обобщая данную работу, можно выделить следующие результаты:

1. Свойства безопасности информации (конфиденциальность, доступность, целостность) можно рассматривать как динамические характеристики с обратной связью.
2. Введена динамическая характеристика безопасности системы и ее показатель – защищенность системы D.
3. Построена линейная система динамических уравнений с обратной связью, которая объединяет такие понятия информационной системы, как угрозы безопасности информации, размер системы, мероприятий по защите информации, защищенность системы, количество информации, конфиденциальность. Выполнен анализ системы уравнений.
4. Выполнена оценка поведения системы при разных значениях коэффициентов угроз, обратной связи размера системы, защищенности, угроз безопасности информации.
5. Сделан вывод о том, что линейная система уравнений имеет стационарную позицию, следующую из связи между защищенностью системы, угрозами безопасности информации и количеством информации.
6. Предложен способ моделирования, на основании, которого может быть произведена объективная оценка баланса между угрозами безопасности информации, мероприятиями по защите и объемом защищаемой информации.
7. В дальнейшем исследовании планируется построение и анализ более конкретизированных динамических нелинейных моделей для конфиденциальности, целостности, доступности.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбылев А. Л. Программный комплекс для автоматизированной генерации организационно-распорядительных документов по защите информации в критических инфраструктурах. Информационные и математические технологии в науке и управлении. Том 3. 2016. Т. 3. С. 185-191.
2. Горбылев А. Л. Адаптированная модель угроз безопасности информации в ключевых системах информационных инфраструктур. Сборник статей международной научно-практической конференции АВТОМАТИЗАЦИЯ: ПРОБЛЕМЫ, ИДЕИ, РЕШЕНИЯ 8 декабря 2017 года. ОМЕГА САЙНС. г. Уфа. Т. 1 С. 35-43.
3. Бондарь И. В. Методика построения модели угроз безопасности информации для автоматизированных систем. Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнева. 2012. С. 7-10.
4. Кубарев А. В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков. Вопросы кибербезопасности. № 2. 2013.
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена заместителем директора ФСТЭК России 15.02.2008.
6. Газизов Т.Т., Мытник А.А., Бутаков А.Н. Типовая модель угроз безопасности персональных данных для информационных систем автоматизации учебного процесса // Доклады ТУСУР. 2014. № 2 (32). С. 47–50.
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14.02.2008.
8. Конев А. А. Подход к построению модели угроз защищаемой информации. Математическое обоснование и теоретические аспекты информационной безопасности. Доклады ТУСУР. 2012. № 1 (25). Ч. 2. С. 34-39.
9. Марков А. С. Фадин А. А. Организационно-технические проблемы защиты от целевых вредоносных программ типа stuxnet. Вопросы кибербезопасности. 2013.
10. Новохрестов А.К., Конев А.А., Шелупанов А.А., Егошин Н.С. Модель угроз безопасности информации и ее носителей // Вестник Иркутского государственного технического университета. 2017. Т. 21. № 10. С. 93–104. DOI: 10.21285/1814-3520-2017-12-93-104.

11. Душкин А.В., Демченков А.В. Аналитическая модель оценки эффективности обеспечения защиты данных от угроз нарушения целостности в информационных системах // Вестник Воронежского института МВД России. 2015. № 1. С. 87–95.
12. Бурькова Е.В. Задача оценки защищенности информационных систем персональных данных // Вестник Чувашского университета. 2016. № 1. С. 112–118.
13. Ступина А.А., Золотарев А.В. Сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем. Вестник СибГАУ. 2012. № 4 (44). С. 56–61.
14. Новохрестов А.К., Никифоров Д.С., Конев А.А., Шелупанов А.А. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов // Доклады ТУСУР. 2016. Т. 19. № 3. С. 111–114.
15. Букин Ю. С., Горбылев А. Л. Индивидуально ориентированная модель для имитации популяционно-генетических процессов у видов, населяющих одномерный ареал. Математическая биология и биоинформатика. 2014. Т. 9. № 2, С. 438-452.
16. Зайцев А.С., А.А. Малюк. Системно-динамическое моделирование угрозы кражи интеллектуальной собственности. Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». 2015. № 12 (155). С. 70-91.
17. https://www.securitylab.ru/blog/personal/Business_without_danger/51986.php.
18. Антипов, А. Л.; Труфанов, А. И.. Модель динамической адаптивной иерархической системы информационной безопасности. Безопасность информационных технологий, [S.l.], v. 15, n. 3, p. 76-82, sep. 2008. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/985>. Дата доступа: 11 july 2018.
19. А. И. Труфанов. Балансовая модель производства информационных ресурсов в условиях конкурентной борьбы // Проблемы равновесия и устойчивости в экономических и социальных системах. Сб. науч. тр. Новосибирск, 1999. С. 121-124.
20. A. Antipov, A. Trufanov. Model of the Adaptive Hierarchical Information Security System. Pandemics and Bioterrorism. Transdisciplinary Information Sharing for Decision-Making against Biological Threats. Vol. 62 NATO Science for Peace and Security Series - E: Human and Societal Dynamics. Edited by: A. Trufanov, A. Rossodivita and M. Guidotti - 2010, p. 171 – 177.

REFERENCES:

[1] Gorbylev A. L. Software for automated generation of organizational and administrative documents to information protection in the critical infrastructures. Информационные и математические технологии в науке и управлении. Volume № 3. 2016. pp. 185-191. (in Russian).
[2] Gorbylev A. L. The modified model of threats of information security in the key systems of information infrastructure. Collection of articles of international scientific-practical conference AUTOMATION: PROBLEMS, IDEAS, SOLUTIONS. 8.12.2017. «OMEGA SAJNS». Ufa. Volume № 1 pp.35-43. (in Russian).
[3] Bondar' I. V. Construction method for information security threat models of automated systems. «Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta imeni akademika M. F. Reshetneva». 2012, pp. 7-10. (in Russian).
[4] Kubarev A. V. The classification characteristics based approach to formalization of information systems vulnerabilities. «Voprosy kiberpezopasnosti». №2 2013. (in Russian).
[5] Basic model of threats to personal data security during their processing in information systems of personal data (extract). FSTEC Russia15.02.2008. (in Russian).
[6] Gazizov T.T., Mytnik A.A., Butakov A.N. Generic Model of Security Threats for Personal Data in regard of Information Systems Dedicated to Academic Planning. «Doklady TUSUR». 2014. № 2 (32). С. 47–50. (in Russian).
[7] Methods of determining the actual threats to the security of personal data during their processing in the information systems of personal data. FSTEC Russia. 14.02.2008. (in Russian).
[8] Konev A. A. Approach to creation protected information model. «Doklady TUSUR», №1 (25), part № 2, 2012, pp. 34-39. (in Russian).
[9] Markov A. S. Fadin A. A. Organizational and technical problems of protection againsttargeted malware such as stuxnet. «Voprosy kiberpezopasnosti». 2013. (in Russian).
[10] Novohrestov A.K., Konev A.A., Shelupanov A.A., Egoshin N.S. Information and information carrier security threat model. «Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta». 2017. Т. 21. № 10. С. 93–104. DOI: 10.21285/1814-3520-2017-12-93-104. (in Russian).

[11] Dushkin A.V., Demchenkov A.V. Analytical model for estimation the effectiveness of efficiency data protection from threats of violations integrity in information systems. «Vestnik Voronezhskogo instituta MVD Rossii». 2015. № 1. pp. 87–95. (in Russian).

[12] Bur'kova E.V. The task of assessing the security of information systems of personal data. «Vestnik Chuvashskogo universiteta». 2016. № 1.pp. 112–118. (in Russian).

[13] Stupina A.A., Zolotarev A.V. Comparative analysis of methods for solution of automatised systems protection estimation problem. «VestnikSibGAU». 2012. № 4 (44). p 56–61. (in Russian).

[14] Novohrestov A.K., Nikiforov D.S., Konev A.A., Shelupanov A.A. Model of threats to automatic system for commercial accounting of power consumption. « Doklady TUSUR ». 2016.V. 19. № 3. pp. 111–114. (in Russian).

[15] Bukin YU. S., Gorbylev A. L. An Individual-Based Model to Simulate Genetic Processes in Populations of Species Inhabiting One-Dimensional Area. Mat. Biolog. Bioinform, 2014, Volume 9, issue2, pp. 438–452. (in Russian).

[16] Zajcev A.S., A.A. Malyuk. System dynamics modeling of threat of intellectual property theft. «Vestnik RGGU». «Informatika. Zashchita informacii i informacionnaya bezopasnost». 2015. № 12 (155), pp. 70-91. (in Russian).

[17] https://www.securitylab.ru/blog/personal/Business_without_danger/51986.php.

[18] Antipov A.L., Trufanov A.I. Model of dynamic active hierarchical information security system. IT Security (Russia), [S.l.], v. 15, n. 3, p. 76-82, sep. 2008. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/985>. Date accessed: 11 july 2018. (in Russian).

[19] Trufanov A.I. Balance model for the production of information resources in a competitive environment. «Problemy ravnovesiya i ustojchivosti v ehkonomicheskih i social'nyh sistemah». «Sbornik nauchnyh trudov» Novosibirsk, 1999. pp. 121-124. (in Russian).

[20] A. Antipov, A. Trufanov. Model of the Adaptive Hierarchical Information Security System. Pandemics and Bioterrorism. Transdisciplinary Information Sharing for Decision-Making against Biological Threats. Vol. 62 NATO Science for Peace and Security Series - E: Human and Societal Dynamics. Edited by: A. Trufanov, A. Rossodivita and M. Guidotti - 2010, p. 171 – 177.

Поступила в редакцию - 16 июня 2018 г. Окончательный вариант –23 августа2018 г.
Received –June 16, 2018. The final version – November August 23, 2018.