УДК 004.056.53

Н. В. Евглевская, А. А. Привалов, Е. В. Скуднева
Петербургский государственный университет путей сообщения
Императора Александра I

МАРКОВСКАЯ МОДЕЛЬ КОНФЛИКТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ С СИСТЕМОЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ НАРУШИТЕЛЯ

Автоматизированная система обработки информации и управления (АСОИУ) является сложной организационно-технической системой, в которой наряду с целевым процессом передачи информации реализуется и технологический процесс управления сетевыми ресурсами и качеством предоставляемых услуг электросвязи. Нарушение этого технологического процесса может привести к отказу самой АСОИУ. В статье рассмотрена марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя. В данной модели нарушитель предпринимает серии согласованных атак, которые приводят к изменению состояния АСОИУ. Восстановлением АСОИУ управляет автоматизированная подсистема администрирования безопасности информации.

марковская модель, автоматизированная система обработки информации и управления (АСОИУ), интенсивность потоков перехода.

Введение

Обеспечение безопасности информации является весьма важным аспектом развития современного общества. В связи с тем, что в АСОИУ обрабатывается и хранится конфиденциальная и секретная информация, данная проблема актуальна при проектировании и эксплуатации АСОИУ [1].

Сложность обеспечения устойчивой работы современных АСОИУ в последнее время возросла из-за участившихся деструктивных информационных воздействий, реализуемых нарушителями, целью которых, как правило, является главный производственный процесс, реализуемый на поражаемом объекте.

Достаточно вспомнить о компьютерном черве Stuxnet и вирусе Shamoon, посредством которых было оказано воздействие на закрытые телекоммуникационные сети центра по обогащению ядерного топлива в Иране и в Саудовской Аравии [2]. В сентябре 2010 г. вирусом Stuxnet была заражена компьютерная система ядерной программы Ирана. 15 августа 2012 г. компьютерная сеть нефтяной компании Saudi Arabian Oil Company (Saudi Aramco) подверглась атаке вируса Shamoon. Попав на компьютер, Shamoon пытается похитить важную информацию, после чего стереть главную загрузочную запись. При этом дальнейшее использование операционной системы становится невозможным.

Анализ показывает, что информационные воздействия на АСОИУ реализуются нарушителем на основании данных, добываемых с использованием средств компьютерной, акустической и ПЭМИН-разведок, которым, в свою очередь, противодействует входящая в структуру АСОИУ подсистема администрирования безопасности информации.

Известны модели, которые ориентированы на определение вероятностно-временных параметров системы деструктивных воздействий нарушителя [2, 3], а также системы управления безопасностью АСОИУ. Однако эти модели не позволяют совместно согласо-

ванно оценить возможности указанных систем, взаимодействующих при информационном противоборстве. Поэтому для выработки требований к подсистемам администрирования безопасности информации представляет практический интерес создание математической модели конфликта АСОИУ с системой деструктивных воздействий нарушителя.

1 Постановка задачи

Пусть имеется АСОИУ, в которой циркулирует, обрабатывается и хранится конфиденциальная информация. Указанная система функционирует в условиях атак нарушителя на охраняемые сведения, утрата которых может привести к существенному экономическому, экологическому или иному ущербу. Под атакой здесь понимается совокупность согласованных по месту, времени и цели программно-аппаратных воздействий со стороны нарушителя на элементы АСОИУ для нанесения указанной системе существенного ущерба или вывода ее из строя.

Восстановлением АСОИУ и нейтрализацией последствий атак нарушителя управляет автоматизированная подсистема администрирования безопасности информации (АПАБИ).

Реализация нарушителем атак на АСОИУ приводит к изменению ее состояния, которое может быть зафиксировано оператором АПАБИ. При этом под состоянием будем понимать число атак, успешно реализованных нарушителем. Процесс восстановления безопасного и/или работоспособного состояния АСОИУ приводит к изменению пространства параметров, наблюдаемых системой информационного противоборства, и нарушитель реализует следующую атаку на АСОИУ. Далее описанный процесс возобновляется.

Функции распределения времени вскрытия системы и реализации атаки нарушителем [2], а также длительности цикла управления АСОИУ со стороны администратора службы безопасности [3] имеют вид

$$F_{\text{РА}}(t) = \sum_{k=1}^{n} \frac{h(s_k)}{g'(s_k)} \cdot \frac{1 - e^{s_k t}}{-s_k};$$
$$F_{\text{УАС}}(t) = \sum_{i=1}^{m} \frac{f(s_i)}{\varphi'(s_i)} \cdot \frac{1 - e^{s_i t}}{-s_i}. \quad (1)$$

Требуется определить вероятность и время пребывания АСОИУ в состоянии безопасности.

2 Решение

Положим, что рассматриваемая АСОИУ имеет n возможных состояний, и представим описанный в постановке задачи процесс в виде графа состояний (рис. 1).

При этом:

• s_1 – состояние безопасности информации в АСОИУ;

• s_2 – состояние АСОИУ, обусловленное успешной реализацией технической разведки и атаки нарушителем; интенсивность перехода в это состояние равно $\lambda_{12}(t)$;

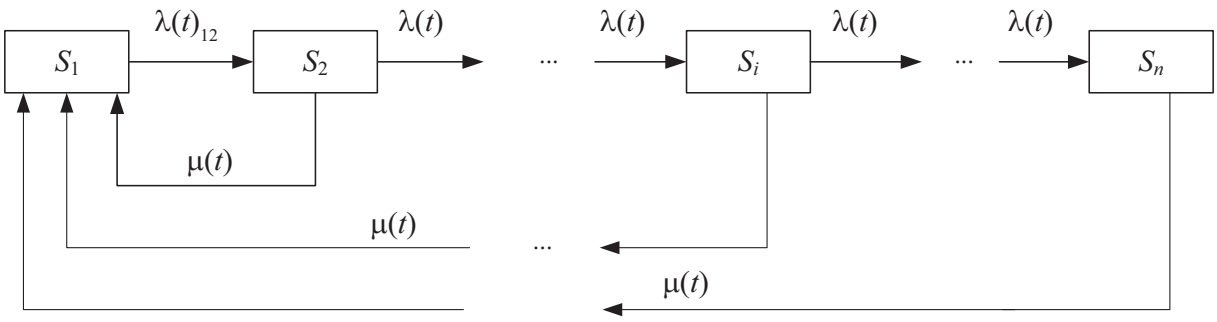


Рис. 1. Размеченный граф состояний АСОИУ

…

• s_i – состояние, в которое переходит АСОИУ в результате успешной реализации $(i-1)$-й атаки нарушителем с интенсивностью $\lambda(t)$;

…

• s_n – состояние, в которое переходит АСОИУ в результате успешной реализации $(n-1)$-й атаки нарушителем с интенсивностью $\lambda(t)$.

На АСОИУ, пребывающую в состоянии s_2, …, s_i, ..., s_n, воздействует поток восстановлений, имеющий интенсивность $\mu(t)$ и переводящий ее в состояние безопасности s_1.

Составим систему уравнений Колмогорова [4].

$$\left|\begin{array}{l}
\dfrac{dP_1(t)}{dt} = \mu(t)\sum\limits_{k=2}^{n} P_k(t) - P_1(t)\lambda(t)_{12}, \\
\dfrac{dP_2(t)}{dt} = P_1(t)\lambda(t)_{12} - P_2(t)\lambda(t) - \\
-P_2(t)\mu(t), \\
\ldots \\
\dfrac{dP_i(t)}{dt} = P_{(i-1)}(t)\lambda(t) - P_i(t)\mu(t) - \\
-P_i(t)\lambda(t), \\
\ldots \\
\dfrac{dP_n(t)}{dt} = P_{(n-1)}(t)\lambda(t) - P_n(t)\mu(t).
\end{array}\right| \quad (2)$$

Начальными условиями являются:

$P_1(0) = 1$; $P_2(0) = 0$;

$\ldots P_i(0) = 0$; $\ldots P_n(0) = 0$;

$\sum\limits_{k=1}^{n} P_k(t) = 1, (i = 1, 2, ..., n)$.

Данная система дифференциальных уравнений может быть решена любым известным в математике методом.

С учетом (1) определим интенсивности потоков перехода АСОИУ из одного состояния в другое:

$$\left|\begin{array}{l}
\lambda_{(12)}(t) = \dfrac{f_{\text{РА}}(t)}{1 - F_{\text{РА}}(t)} = \\
= \dfrac{\sum\limits_{k=1}^{n} \dfrac{h(s_k)e^{s_k t}}{g'(s_k)}}{1 - \sum\limits_{k=1}^{n} \dfrac{h(s_k)}{g'(s_k)} \cdot \dfrac{1 - e^{s_k t}}{-s_k}} = \dfrac{\sum\limits_{k=1}^{n} \dfrac{h(s_k)}{g'(s_k)} s_k e^{s_k t}}{\sum\limits_{k=1}^{n} \dfrac{h(s_k)}{g'(s_k)} e^{s_k t}}; \\
\mu(t) = \dfrac{f_{\text{УАС}}(t)}{1 - F_{\text{УАС}}(t)} = \\
= \dfrac{\sum\limits_{i=1}^{m} \dfrac{f(s_i)e^{s_i t}}{\varphi'(s_i)}}{1 - \sum\limits_{i=1}^{m} \dfrac{f(s_i)}{\varphi'(s_i)} \cdot \dfrac{1 - e^{s_i t}}{-s_i}} = \dfrac{\sum\limits_{i=1}^{m} \dfrac{f(s_i)}{\varphi'(s_i)} s_i e^{s_i t}}{\sum\limits_{i=1}^{m} \dfrac{f(s_i)}{\varphi'(s_i)} e^{s_i t}}.
\end{array}\right| \quad (3)$$

Анализ результатов информационного воздействия на реальные автоматизированные системы [5] показывает, что для осуществления деструктивного воздействия нарушителю достаточно успешно реализовать не более трех атак. Поэтому без потери общности допустим, что $n = 4$.

Тогда граф состояний примет вид, представленный на рис. 2.

Тогда система уравнений (2) преобразуется к виду:

$$\frac{dP_1(t)}{dt} = P_2(t)\mu(t) + P_3(t)\mu(t) + P_4(t)\mu(t) - P_1(t)\lambda(t)_{12};$$

$$\frac{dP_2(t)}{dt} = P_1(t)\lambda(t)_{12} - P_2(t)\lambda(t) - P_2(t)\mu(t);$$

$$\frac{dP_3(t)}{dt} = P_2(t)\lambda(t) - P_3(t)\lambda(t) - P_3(t)\mu(t);$$

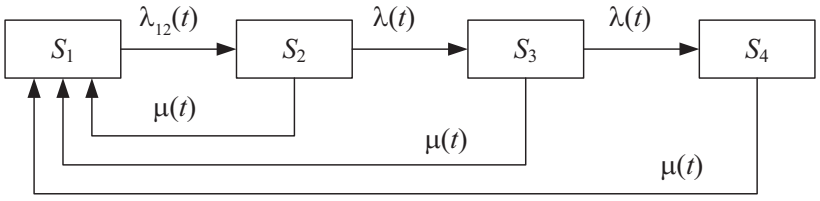


Рис. 2. Размеченный граф состояний АСОИУ при $n = 4$

$$\frac{dP_4(t)}{dt} = P_3(t)\lambda(t) - P_4(t)\mu(t).$$

$$\sum_{i=1}^{4} P_4(t) = 1.$$

Начальные условия:

$P_1(0) = 1, P_2(0) = P_3(0) = P_4(0) = 0.$

Решениями системы дифференциальных уравнений являются вероятности пребывания АСОИУ в состояниях $s_1, \ldots s_4$, т. е.:

$$P_1(t) = \frac{\mu(t)}{\mu(t) + \lambda_{12}(t)} + \\ + (1 - \frac{\mu(t)}{\mu(t) + \lambda_{12}(t)}) e^{-(\mu(t)+\lambda_{12}(t))t}; \quad (4)$$

$$P_2(t) = -\frac{A(t)}{\alpha(t)} - \frac{\Lambda(t)}{\alpha(t) - M(t)} e^{M(t)t} + \\ + \left[\frac{A(t)}{\alpha(t)} + \frac{\Lambda(t)}{\alpha(t) - M(t)} \right] e^{\alpha(t)t}; \quad (5)$$

$$P_3(t) = \frac{A(t) \cdot \lambda(t)}{\alpha^2(t)} [1 + (\alpha(t)t - 1) e^{\alpha(t)t}] + \\ + \Lambda(t)\lambda(t) \times \\ \times \frac{e^{M(t)t} - [1 + (M(t) - \alpha(t))t] e^{\alpha(t)t}}{(M(t) - \alpha(t))^2}; \quad (6)$$

$$P_4(t) = 1 - P_1(t) - P_2(t) - P_3(t), \quad (7)$$

где

$$A(t) = \frac{\mu(t) \cdot \lambda_{12}(t)}{\mu(t) + \lambda_{12}(t)};$$

$$\Lambda(t) = \lambda_{12}(t)(1 - \frac{\mu(t)}{\mu(t) + \lambda_{12}(t)});$$

$$M(t) = -(\mu(t) + \lambda_{12}(t));$$

$$\alpha(t) = -(\lambda(t) + \mu(t)).$$

Время, в течение которого АСОИУ будет находиться в состоянии безопасности, можно определить подстановкой в (4) вместо $P_1(t)$ значения уровня $P_{\text{треб}}$, предъявляемого к системе требований по безопасности. Полагая $\mu(t) = \text{const}$ и $\lambda_{12}(t) = \text{const}$, получим

$$T = \frac{-\ln(\frac{-\mu + P_{\text{треб}} \cdot \mu + P_{\text{треб}}}{\lambda_{12}})}{(\mu + \lambda_{12})}, \quad (8)$$

где $P_{\text{треб}}$ – требуемое значение вероятности пребывания системы в состоянии безопасности [6].

Таким образом, поставленная задача решена.

3 Результаты моделирования

С использованием (3), а также результатов [2, 3] было установлено, что интенсивность перехода АСОИУ, обусловленная успешной реализацией технической разведки и атаки нарушителем $\lambda_{12}(t)$, и интенсивность потока восстановлений $\mu(t)$, переводящего ее в состояние безопасности, изменяются в пределах $\lambda_{12}(t) = 0{,}05–0{,}07$ (1/мин.); $\mu(t) = 0{,}03–1$ (1/мин.). Это дает основание полагать, что длительность ведения разведки нарушителем изменяется от 5 до 15 мин.; длительность реализации атаки – в пределах 3–8 мин.; длительность восстановления АСОИУ в зависимости от глубины ее поражения – 1–30 мин.

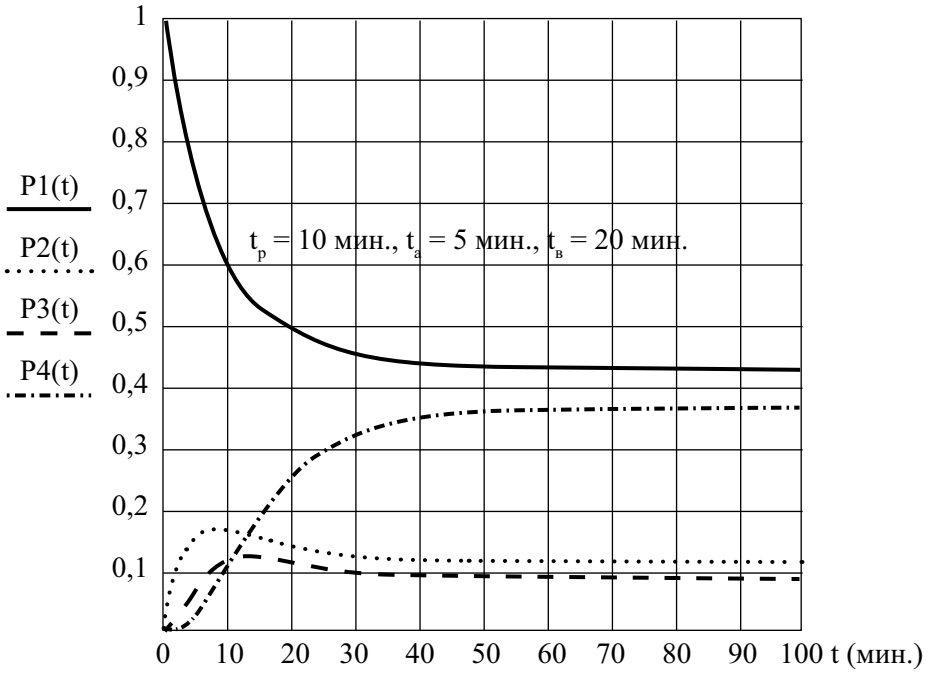
По формуле (8) рассчитано время, в течение которого АСОИУ будет пребывать в состоянии безопасности s_1.

На рис. 3 представлены графики вероятностей пребывания АСОИУ в состояниях s_i при разном времени проведения разведки, атаки нарушителем, а также восстановления системы.

Заключение

Анализ полученных результатов позволяет сделать следующие выводы.

Разработанная модель работоспособна, чувствительна к изменению исходных данных, адекватно отображает процесс разведки и атак нарушителя, а также процесс восстановления безопасного состояния АСОИУ.



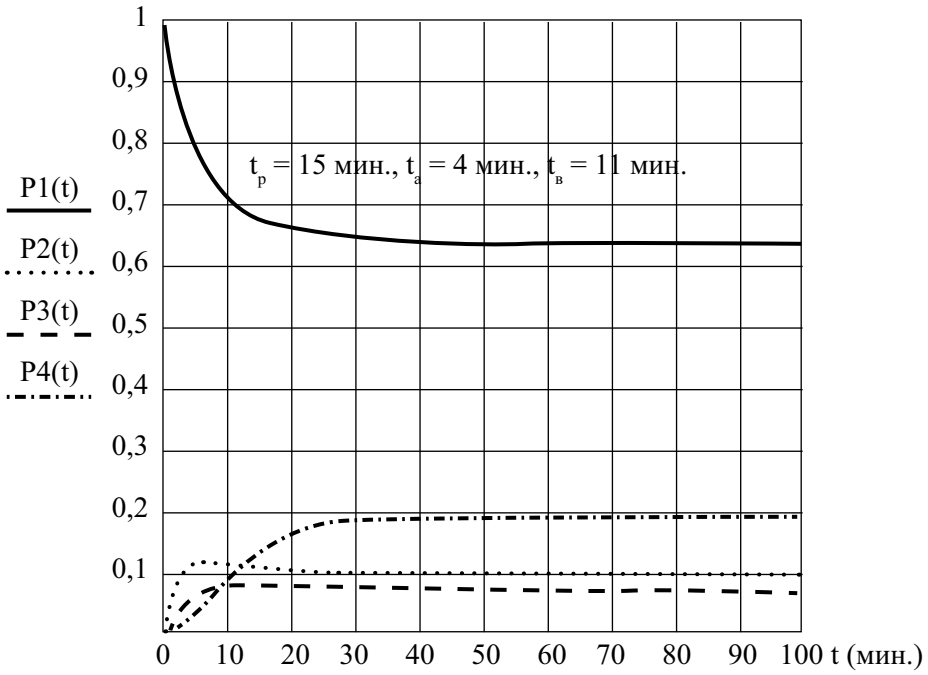
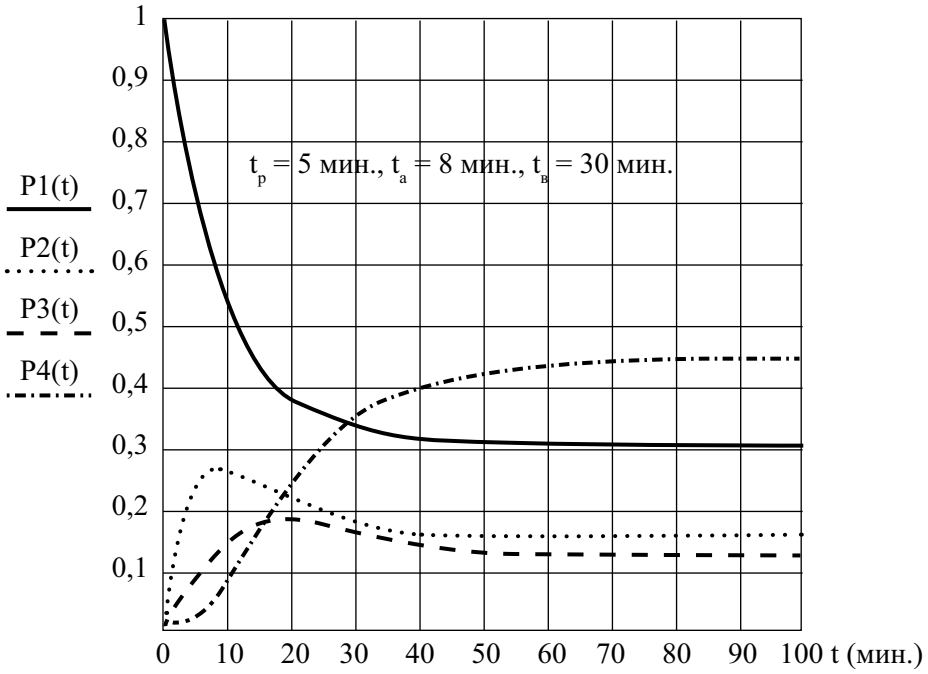


Рис. 3. Графики вероятностей пребывания АСОИУ в состояниях s_i при различном времени проведения разведки, атаки со стороны нарушителя и восстановления системы



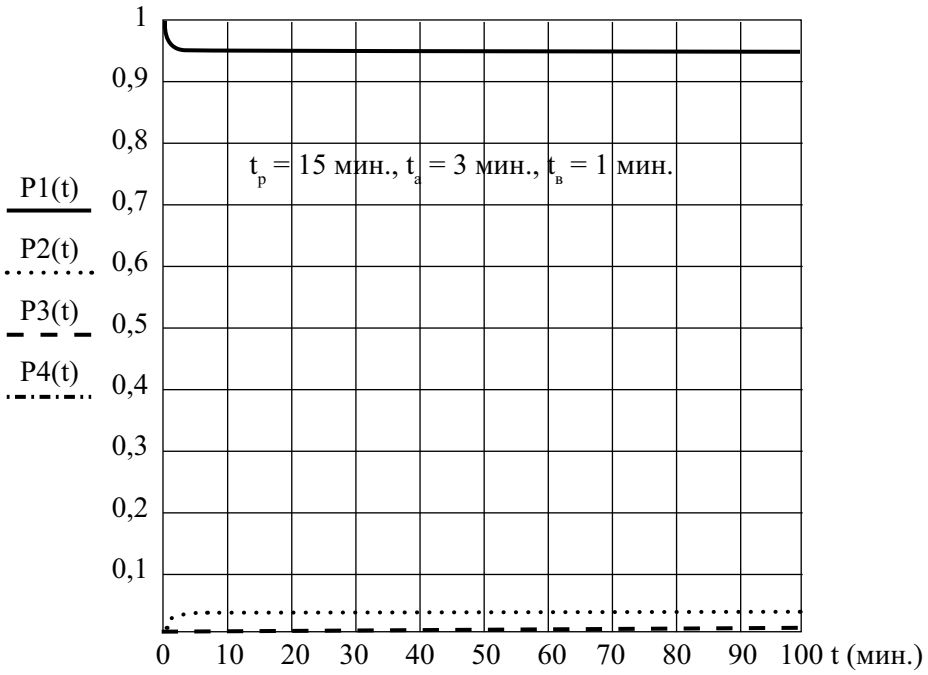


Рис. 3. Графики вероятностей пребывания АСОИУ в состояниях s_i при различном времени проведения разведки, атаки со стороны нарушителя и восстановления системы (окончание)

Полученные в ходе моделирования значения среднего времени пребывания АСОИУ в состоянии безопасности позволяют на этапе технического проектирования системы определять рациональную периодичность и глубину контроля безопасности информации за счет использования вычисленных значений в качестве критериальных.

Достижение уровня предъявляемых требований по безопасности может быть обеспечено при длительности цикла управления АСОИУ, не превышающим одной десятой длительности времени подготовки и реализации нарушителем атаки на защищаемую систему, т. е. $\mu^{-1} \leq 0{,}1\lambda^{-1}$.

Следует ожидать, что на защищаемую систему нарушитель будет оказывать не одиночные воздействия, а серии согласованных атак. При этом возможность успешной реализации атаки остается практически при любой системе защиты, если мероприятия по защите неадекватны и не согласованы с действиями нарушителя. Отсюда возникает задача создания такой системы администрирования безопасности, которая имеет в своем составе подсистему поддержки принятия решений по выбору мероприятий и мер защиты, обеспечивающую оценку, прогнозирование и минимизацию возможностей нарушителя по реализации атак. К сожалению, отечественные стандарты в области безопасности информации (руководящие документы, ГОСТы и т. д.) и имеющийся в них методический аппарат не позволяют в полной мере реализовать перечисленные выше функции.

Таким образом, предложенная модель позволяет разработать методику оценки кибербезопасности автоматизированных систем обработки информации и управления, функционирующих в условиях информационного противоборства.

Библиографический список

1. **Вероятностные** модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления / П. И. Титубалин, В. С. Моисеев. – Казань : Школа, 2008. – 144 с.

2. **Модель** процесса подготовки злоумышленника к информационному воздействию на автоматизированные системы управления железнодорожным транспортом / Н. В. Евглевская, А. А. Привалов, Ал. А. Привалов // Бюл. результатов науч. исследований. – 2012. – № 5 (4). – С. 17–26.

3. **Об оценке** длительности цикла управления телекоммуникационной сетью ОАО «РЖД» / А. А. Привалов, А. П. Вандич, Д. А. Полторацкий // Материалы V междунар. конгресса «Цели развития тысячелетия и инновационные принципы устойчивого развития арктических регионов». – СПб. : Арктич. обществ. академия наук, 2012. – С. 92–95.

4. **Теория** случайных процессов и ее инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М. : Высш. шк., 2000. – 383 с.

5. **Информационное** противоборство в войнах и вооруженных конфликтах / В. С. Киреев, Р. В. Максимов, А. А. Погорелов и др. – СПб. : ВАС, 2005. – 120 с.

6. **ГОСТ РВ 51987-2002.** Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения. – М. : Госстандарт России, 2001. – 53 с.