МНОГОУРОВНЕВАЯ ЛОГИКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ОБМЕНА В ВЕДОМСТВЕННОЙ СИСТЕМЕ УПРАВЛЕНИЯ

Потапчик Н. Н.[1], Пылинский М. В.[2]

DOI:10.21681/3034-4050-2025-4-10-21

Ключевые слова: *информационное превосходство, телекоммуникационная подсистема, информационно-техническое воздействие, дестабилизирующий фактор, безопасность информационного обмена, свойство стойкости, общий логико-вероятностный метод.*

Аннотация

Цель работы: *состоит в разработке многоуровневой логико-вероятностной модели информационного обмена со свойством стойкости в ведомственной системе управления.*

Метод исследования: *проведенное исследование основано на общенаучных методах: анализа, синтеза, абстрагирования, обобщения, моделирования, индукции, дедукции. В качестве ключевого метода обоснованно выбран и использовался общий логико-вероятностный метод, а также теория вероятностей.*

Результаты исследования: *разработана многоуровневая логико-вероятностная модель информационного обмена со свойством стойкости, включающая частные модели исследуемого процесса в уязвимых подсистемах и элементах телекоммуникационной подсистемы ведомственной системы управления. Представленная модель позволяет получить уравнения вероятностных функций свойства стойкости информационного обмена, подверженного воздействию комплекса дестабилизирующих факторов информационно-технического воздействия, установить новые количественно обоснованные зависимости между входными и выходными параметрами и оценить стойкость исследуемого процесса в ведомственной системе управления. Доказана адекватность разработанной модели. В основной части статьи с использованием представленной модели произведен расчет и оценка вероятностно-временных характеристик свойства стойкости информационного обмена в информационном направлении ведомственной системы управления. Результаты оценки указывают на необходимость разработки организационно-технических мероприятий, направленных на обеспечение безопасности информационного обмена в ведомственных системах управления.*

Научная новизна: *представленная многоуровневая логико-вероятностная модель позволяет: выявить закономерности динамики прохождения информационного обмена в ведомственных системах управления; использовать стратифицированный подход, который на основе базовой логико-вероятностной модели информационного обмена, позволяет создавать схемы функциональной целостности исследуемого процесса любого уровня декомпозиции в системах управления различной топологической структуры; учитывать динамику информационного противоборства посредством задания временных параметров дестабилизирующих факторов информационно-технического воздействия.*

Введение

В современных условиях на потенциальные угрозы и вызовы динамично изменяющейся обстановки адекватнее и быстрее сможет реагировать тот участник, управление которого будет более эффективным [1]. Основным мероприятием организации управления является создание системы управления (СУ), важнейшим элементом которой является информационная система (ИС), выполняющая задачи информационного обеспечения процесса управления. В информационных процессах, протекающих в СУ, можно выделить две сугубо отличающиеся по целям и выполняемым задачам компоненты: процесс доставки информации (информационный обмен)

1 Потапчик Николай Николаевич, адъюнкт кафедры связи факультета связи и автоматизированных систем управления Военной академии Республики Беларусь, г. Минск, Республика Беларуссия. E-mail: nikpotapchik89@gmail.com

2 Пылинский Максим Валерьевич, доктор военных наук, профессор, начальник кафедры связи факультета связи и автоматизированных систем управления Военной академии Республики Беларусь, г. Минск, Республика Беларусь. E-mail: pylinskii.maksim@mail.ru

от субъекта управления к объекту управления и процессы обработки, преобразования и использования полученной информации при решении управленческих задач[3]. Как следствие, ИС ведомственной СУ представляет собой совокупность взаимосвязанных телекоммуникационной подсистемы (ТП) и подсистемы обработки информации.

Из всей совокупности информационных процессов, реализуемых ИС, главенствующая роль отводится информационному обмену между распределенными в пространстве объектами управления, что объясняется неизбежностью разрушения самой СУ при ослаблении или потери информационных связей между ее элементами, а также зависимостью уровня управления от объема передаваемой информации [2]. Удовлетворение потребностей ведомственной СУ в передаче заданного объема информации обеспечивается функционированием ее ТП.

Особенностями построения современных ведомственных ТП является использование в качестве транспортной составляющей сети электросвязи общего пользования (СЭОП) [3], а также применение технологий, средств связи (СС) и программного обеспечения (ПО) иностранного производства, имеющих потенциальные уязвимости и незадекларированные возможности [4]. Данные обстоятельства существенно повышают возможности противоборствующей стороны (силовых структур иностранных государств, террористических организаций и отдельных злоумышленников) по осуществлению информационно-технического воздействия (ИТВ), направленного на завоевание и удержание информационного превосходства в информационном пространстве [5–7]. К существенным факторам ИТВ, создающим угрозы процессу обмена информацией в ведомственной СУ, относятся программно-техническое воздействие (ПТВ) и электронное воздействие (ЭВ) преднамеренными радиоэлектронными помехами (ПРП) [2, 6].

Проведенный анализ фактов реализации ПТВ в различных странах мира показал, что в большинстве случаев для нарушения (блокирования) информационного обмена в системах управления различного назначения использовались комплексные кибератаки «Отказ в обслуживании, DDoS-атака» (ККА), которые в своем составе включают этапы ведения сетевой разведки (СР) и реализации распределенной кибератаки «Отказ в обслуживании, DDoS-атака» [8]. Массовое применение указанных ККА вызвано высокой эффективностью, а также относительной простотой реализации и невысокой стоимостью осуществления [9].

Безопасность является одним из главных требований, предъявляемых СУ к информационному обмену. Указанное свойство характеризует способность исследуемого процесса противостоять несанкционированному получению, уничтожению и изменению информации, передаваемой (принимаемой) с использованием технических СС, а также противостоять нарушению обмена информацией вследствие оказания воздействий всех видов на ТП и ее элементы [2]. Из приведенного определения следует, что безопасность информационного обмена отражает состояние защищенности информации и процесса ее передачи в ТП СУ и характеризуется набором следующих свойств: конфиденциальностью и целостностью передаваемой информации, а также стойкостью информационного обмена. Показателями конфиденциальности и целостности являются коэффициент закрытия $K_{\text{з ИО}}$ и вероятность ввода ложной информации $P_{\text{вли}}$. Показателями стойкости информационного обмена – коэффициент стойкости $K_{\text{ст ИО}}$, представляющий собой отношение времени прохождения информационного обмена с вероятностью не меньше требуемой, к суммарному времени обеспечения управления, а также функция стойкости $F_{\text{ст ИО}}(t)$, имеющая смысл распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) в СУ и отображающую динамику изменения стойкости информационного обмена во времени с учетом воздействия комплекса дестабилизирующих факторов (ДФ) [2].

Постановка задачи

Проведенный анализ трудов, посвященных исследованию информационных процессов, протекающих в ведомственных СУ, выявил отсутствие исчерпывающей, не требующей уточнения и пересмотра модели информационного обмена со свойством стойкости, позволяющей выявить закономерности динамики прохождения исследуемого процесса в условиях воздействия комплекса ДФ ИТВ.

3 Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 184 с.

С учетом вышеизложенного актуализируется задача по созданию такой модели, включающей частные модели информационного обмена в уязвимых подсистемах и элементах ТП, и позволяющей получить уравнения вероятностных функций свойства стойкости, отражающих способность информационного обмена противостоять нарушению (блокированию) в результате воздействия комплекса ДФ ИТВ, установить новые количественно обоснованные зависимости между входными и выходными параметрами и оценить стойкость информационного обмена в соответствии с заданными критериями состояния управления.

Решение задачи

Основным методическим приемом для исследования процесса, реализацию которого обеспечивает структурно-сложная система, является рассмотрение данного процесса в отдельных ее элементах, которые в совокупности обеспечивают выполнение указанного процесса всей системой.

Анализ особенностей построения топологических структур ТП, обеспечивающих передачу заданного объема информации [10], позволил декомпозировать исследуемый процесс в ведомственной СУ на уровни информационного обмена в СС, аппаратной (станции), информационном направлении (ИН) и ТП в целом. Учет функционального аспекта свойства стойкости исследуемого процесса видится особенно важным при сохранении иерархичной структуры уровней декомпозиции информационного обмена в элементах ТП, структурно-логические взаимосвязи которых образуют информационные пути прохождения информации в ведомственной СУ. Нарушение (блокирование) информация в результате воздействия ДФ даже в одном системообразующем элементе в цепи объектов связи ТП, через которые информационного обмена последовательно проходит от субъекта к объекту управления, может привести к снижению степени обеспечения управления, вплоть до его срыва.

На рис. 1 представлена иерархическая структура уровней декомпозиции информационного обмена на примере одного ИН ведомственной СУ, из которой можно сделать вывод, что фундаментом разрабатываемой многоуровневой модели является уровень информационного обмена в СС. Как следствие, указанный уровень декомпозиции принят в качестве базового. Поскольку прохождение информационного обмена в ведомственной СУ определяется структурно-логическими взаимосвязями ее элементов, совокупность моделей исследуемого процесса в условном объекте связи (ОС) позволила создать модели более высоких уровней декомпозиции.

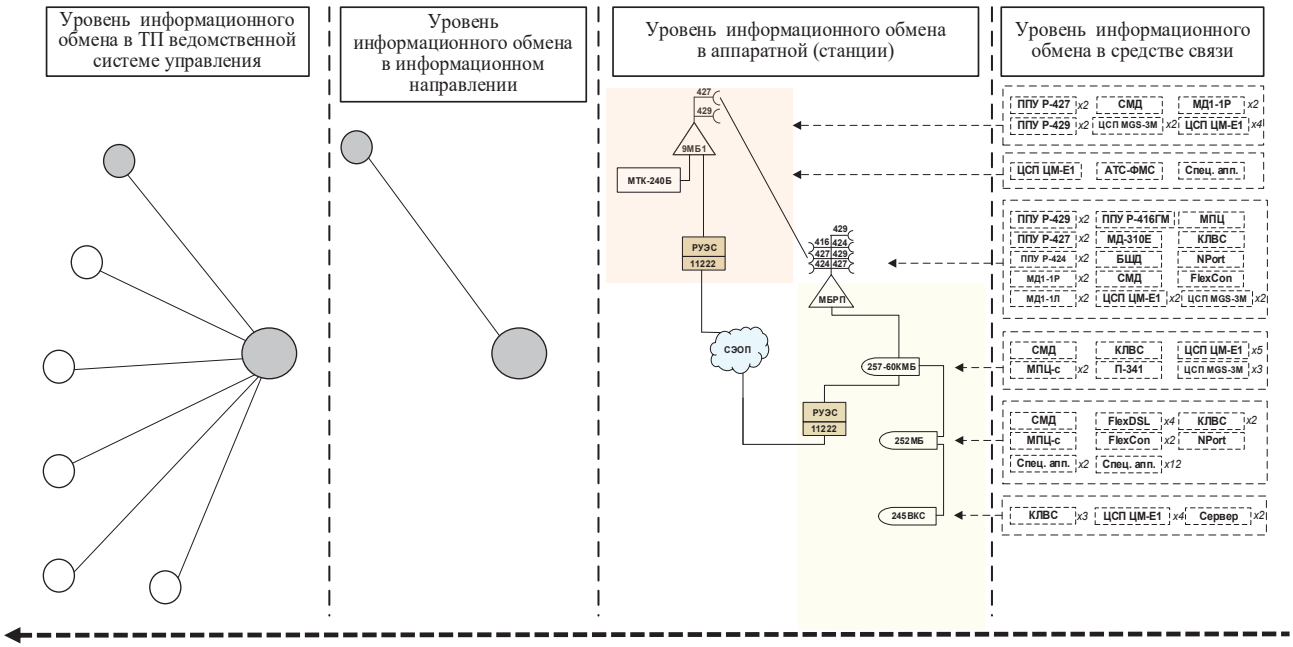

Рис. 1. Иерархичная структура уровней декомпозиции информационного обмена на примере одного информационного направления ведомственной системы управления

Анализ возможностей отечественных и зарубежных методов по решению задач вероятностно-временного моделирования процессов, реализуемых структурно сложными системами, показал, что для решения подобных задач необходимо отдавать предпочтение логико-вероятностным методам. Указанный класс методов позволяет формализовать исходную постановку задачи и создавать модели процесса аналитическими и структурно-логическими средствами, а определение искомых показателей выполняется с использованием средств теории вероятностей. Кроме того, заложенные процедуры преобразования исходных моделей в искомые расчетные математические позволят без дополнительных сложностей алгоритмизировать их с последующей реализацией на электронных вычислительных машинах.

Среди логико-вероятностных методов исследования (методы на основе схем деревьев отказов, деревьев событий, блок-схем, графов состояний и переходов) выделяют общий логико-вероятностный метод (ОЛВМ), создание которого было вызвано необходимостью расширения инструментария указанных методов. Так, по сравнению с другими подобными инструментами ОЛВМ обладает существенными преимуществами[4]:

- ❖ в ОЛВМ уже реализованы все основные возможности как метода деревьев отказов, так и метода блок-схем;
- ❖ реализованная в ОЛВМ функционально полная база логических операций «и», «или» и «не» обеспечивает возможность теоретической разработки и программной реализации методов моделирования и расчетных методик как монотонного, так и немонотонного моделирования процессов различного назначения в структурно сложных системах;
- ❖ ОЛВМ позволяет пользователю выбирать и применять разные подходы (прямой, обратный и их смешанные комбинации) к постановке задач моделирования.

Таким образом, приведенные достоинства позволяют обоснованно выбрать ОЛВМ в качестве универсального средства, наиболее пригодного для решения задач настоящего исследования.

4 Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства: моногр. / В. И. Поленин [и др.]; под ред. проф. А. С. Можаева. – СПб.: НИКА, 2011. 410 с.

В целях решения поставленной задачи с помощью возможностей ОЛВМ была разработана модель информационного обмена со свойством стойкости в условном ОС (базовая модель), подверженного воздействию комплекса ДФ ИТВ (рис. 2).

Для задания прогнозируемого сценария воздействия комплекса ДФ ИТВ в представленную модель введены функциональные вершины 3, 4, которые отражают вероятности появления ПТВ в виде ККА и ЭВ в виде ПРП, и позволяют задавать (изменять) сценарий дестабилизирующего воздействия.

Указанные вершины принимают одно из двух значений булева множества: «1» – при осуществлении события (возникновении ДФ), «0» – при его отсутствии – и являются обеспечивающими по отношению к вершинам 1, 2.

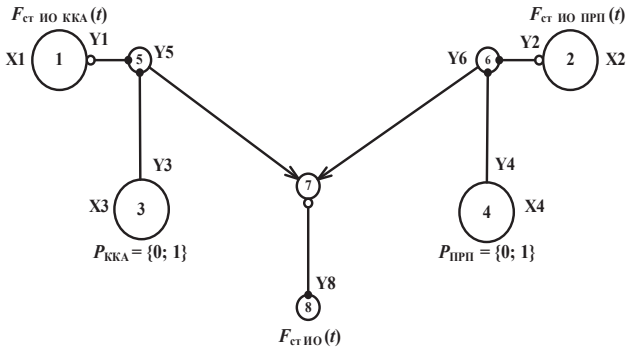

Рис. 2. Модель информационного обмена со свойством стойкости в условном объекте связи

Вершины 1 и 2 отражают функции распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) при воздействии ДФ и отражают его стойкость в условном ОС. В свою очередь фиктивная вершина 8 отражает логическое условие сохранения стойкости информационного обмена в условном ОС.

Логическая функция стойкости информационного обмена в условном ОС описывается равенством

$$Y_{\text{ст ИО}} = x_1 \cdot x_2 \vee \overline{x_3} \cdot x_2 \vee x_1 \cdot \overline{x_4},$$

а вероятностная функция с учетом перехода от вероятностных мер к функциям распределения вероятности времени реализации ДФ – выражением

$$F_{\text{ст ИО}}(t) = F_{\text{ст ИО ККА}}(t) \cdot F_{\text{ст ИО ПРП}}(t) + Q_{\text{ККА}} \cdot Q_{\text{ст ИО ККА}}(t) \cdot F_{\text{ст ИО ПРП}}(t) + Q_{\text{ПРП}} \cdot Q_{\text{ст ИО ПРП}}(t) \cdot F_{\text{ст ИО ККА}}(t),$$

где $F_{\text{ст ИО ККА}}(t)$, $F_{\text{ст ИО ПРП}}(t)$ – функции распределения вероятности времени прохождения информационного обмена без нарушения (блокирования) при воздействии ККА и ПРП; $P_{\text{ККА}}$, $P_{\text{ПРП}}$ – вероятности появления ККА и ПРП; $Q_{\text{ККА}}$, $Q_{\text{ПРП}}$ и $Q_{\text{ст ИО ККА}}(t)$, $Q_{\text{ст ИО ПРП}}(t)$ – величины, обратные $P_{\text{ККА}}$, $P_{\text{ПРП}}$ и $F_{\text{ст ИО ККА}}(t)$, $F_{\text{ст ИО ПРП}}(t)$ соответственно.

Разработанная базовая модель предполагает возможность учитывать и иные ДФ, приводящие к срыву (блокированию) информационного обмена в ведомственной СУ, путем включения в ее структуру дополнительных функциональных вершин, характеризующих свойство стойкости исследуемого процесса в условиях их воздействия.

Для доказательства адекватности представленной модели в ее структуру были введены дополнительные фиктивные вершины (рис. 3). Отражая результаты прямого и обратного подходов к оценке свойства стойкости информационного обмена, фиктивные вершины 9 и 10 являются противоположными по смыслу и образуют полную группу событий, а следовательно, сумма их вероятностей должна быть равна единице, что подтверждают проведенные расчеты по оценке адекватности модели с произвольными исходными данными.

Поскольку аппарат ОЛВМ является математически строгим и позволяет достаточно точно представлять в разрабатываемой модели все существенные логические связи, отношения и зависимости, на основании непротиворечивости полученных результатов и полного

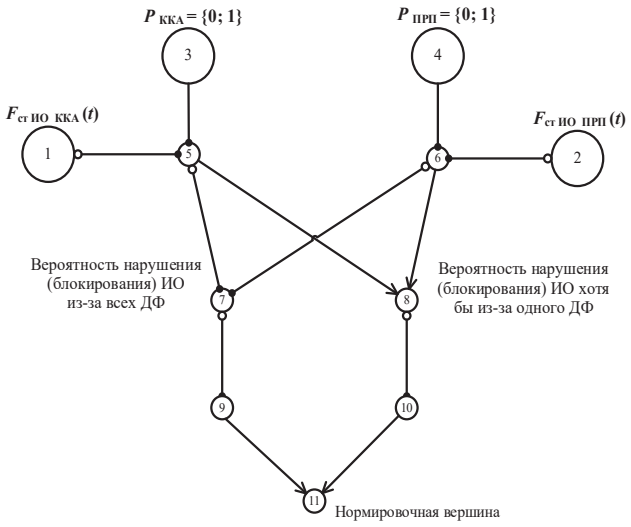

Рис. 3. Модель информационного обмена в условном объекте связи с нормировочной вершиной

подобия эталонному процессу можно утверждать, что базовая модель, а следовательно, и схемы функциональной целостности (СФЦ) информационного обмена более высоких уровней декомпозиции, построенные на ее основе, адекватны моделируемому процессу.

Моделирование информационного обмена более высоких уровней декомпозиции (рис. 1) основывается на идее агрегирования базовой модели в СФЦ информационного обмена в аппаратных (станциях), ИН и ТП ведомственной СУ с учетом структурно-логических взаимосвязей СС, входящих в их состав. Причем любой уровень декомпозиции исследуемого процесса может быть представлен как в виде разработанной базовой модели, так и в виде совокупности взаимосвязанных базовых моделей информационного обмена во вложенных элементах ТП.

В соответствии с приведенной схемой (рис. 4) модель информационного обмена в ведомственной СУ может быть представлена как:

- совокупность СФЦ информационного обмена в ИН, представленных в виде базовой модели (на рис. 4 – переход от блока 1.1 к блоку 2.2), а также в виде совокупности взаимосвязанных СФЦ информационного обмена в аппаратных (станциях), представленных в виде базовой модели (на рис. 4 – переход от блока 1.2 к блоку 3.2);
- совокупность СФЦ информационного обмена в ИН, которые на своем уровне могут быть представлены в виде совокупности взаимосвязанных СФЦ исследуемого процесса в аппаратных (станциях) (на рис. 4 – переход от блока 1.1 к блоку 2.1). Аппаратные (станции) в свою очередь могут быть представлены базовой моделью (на рис. 4 – переход от блока 1.1 к блоку 2.1 с последующим переходом к блоку 3.2), так и совокупностью взаимосвязанных СФЦ информационного обмена в СС, входящих в их состав (на рис. 4 – переход от блока 1.1 к блоку 2.1, далее к блоку 3.1 с последующим переходом к блоку 4.1);
- совокупность взаимосвязанных СФЦ информационного обмена в аппаратных (станциях), которые на своем уровне могут быть представлены совокупностью СФЦ исследуемого процесса в СС, входящих в их состав (на рис. 4 – переход от блока 1.2 к блоку 3.1 с последующим переходом к блоку 4.1).

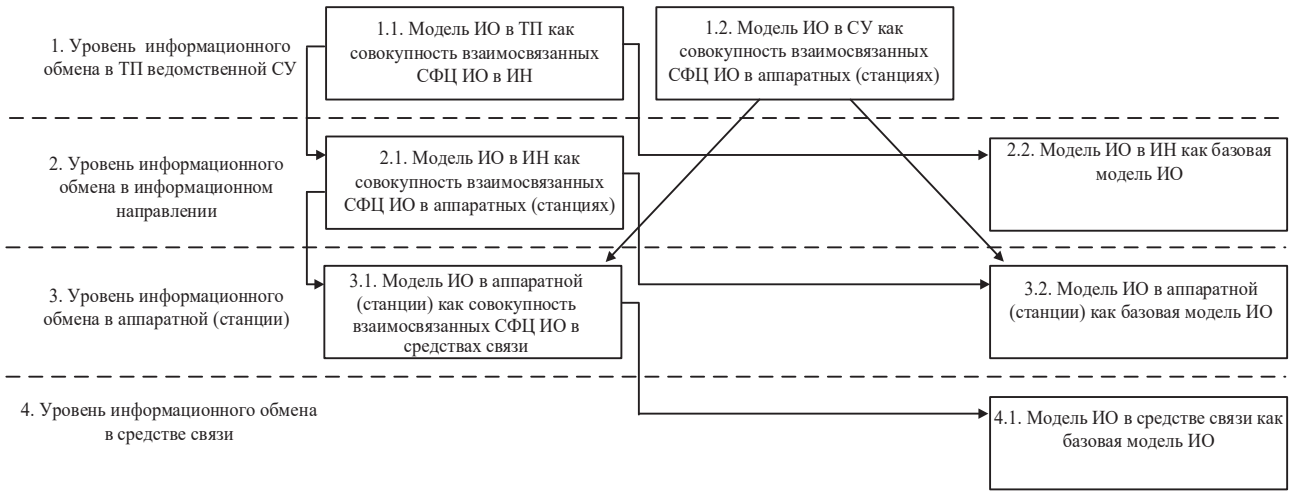

Рис. 4. Возможные варианты представления модели информационного обмена в ведомственной системе управления

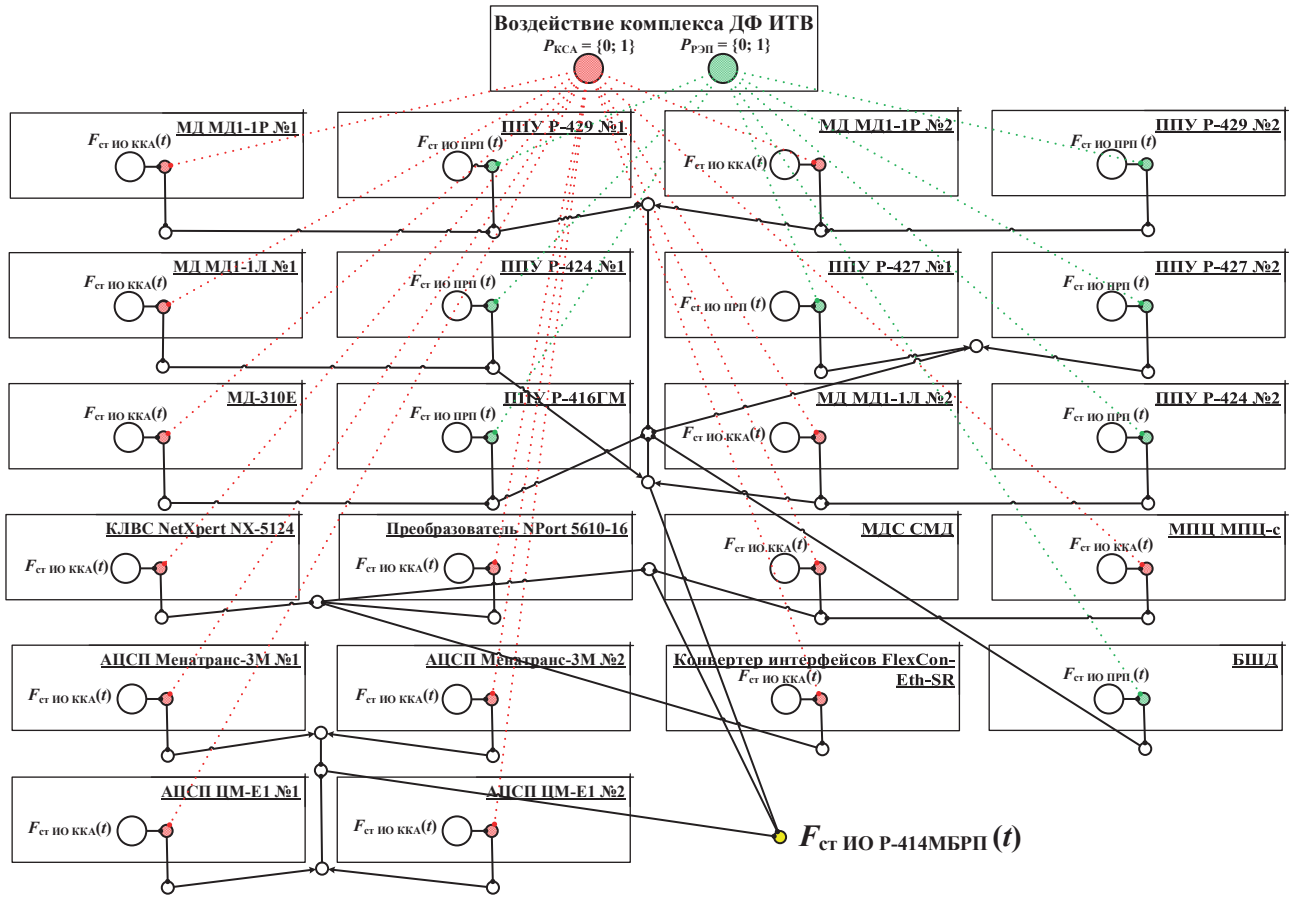

Рис. 5. Модель информационного обмена со свойством стойкости в радиорелейной станции Р-414МБРП

В качестве примера на (рис. 5) приведена модель информационного обмена со свойством стойкости в радиорелейной (РР) станции Р-414МБРП, которая представлена в виде совокупности взаимосвязанных СФЦ исследуемого процесса в СС, входящих в ее состав, которые представлены базовой моделью.

Наиболее точная оценка стойкости информационного обмена в ведомственной СУ обеспечивается посредством использования варианта, при котором осуществляется моделирование исследуемого процесса со свойством стойкости во всех подсистемах и элементах ТП СУ и учитываются все возможные логические взаимосвязи между ними, т. е. цепочка «уровень информационного обмена в ТП ведомственной СУ – уровень информационного обмена в ИН – уровень информационного обмена в аппаратной (станции) – уровень информационного обмена в СС». Такой вариант моделирования целесообразно использовать при достаточном количестве времени, например, в ходе учебной, научно-исследовательской деятельности или проведении опытно-конструкторских работ. При ограниченном временном ресурсе для экспресс-оценки целесообразно использовать менее точные модели, в которых прохождение информационного обмена представлено базовой моделью. При этом следует учитывать, что результаты оценки будут более оптимистичными и менее точными.

Пример расчета вероятностно-временных характеристик (ВВХ) свойства стойкости информационного обмена в ИН ведомственной СУ

Для нахождения ВВХ свойства стойкости информационного обмена в ведомственной СУ, подверженного воздействию комплекса ДФ ИТВ, введены следующие допущения и ограничения:

- вероятность возникновения ДФ ПТВ и ЭВ считалась известной и задана значениями булева множества $P_{ДФi} = \{0; 1\}$ в соответствии с прогнозируемым сценарием ИТВ противоборствующей стороны (рис. 6), разработанного на основе сведений, изложенных в трудах[5];
- исходные данные прогнозируемого сценария ИТВ представлены в таблице 1;
- функции распределения вероятности времени реализации ПТВ в виде ККА и ЭВ в виде ПРП считались известны и рассчитаны для исходных данных, представленных [2];
- время, за которое происходит восстановление информационного обмена в условном ОС после воздействия каждого ДФ, взято и равно $T_в$ = 30 мин;
- для обеспечения передачи информации в ведомственной СУ организовано одно ИН, топологическая структура которого представлена на рис. 7. Информационная взаимосвязь между субъектом и объектом управления обеспечивается функционированием двух направлений связи (НС): РР и проводного (Пр) с использованием цифровых РР станций Р-427 комплексной аппаратной связи Р-409МБ1(КАС) и цифровых систем передачи SHDSL ЦМ-Е1 соответственно.

Требуется с помощью разработанной многоуровневой логико-вероятностной модели

5 а) Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: моногр. СПб.: Наукоемкие технологии, 2017. 546 с.
б) Валецкий О. В. Уроки Ирака. Тактика, стратегия и техника в Иракских войнах США. М.: Издатель Воробьев А. В. 2015. 212 с.
в) Батюшкин С. А. Подготовка и ведение боевых действий в локальных войнах и вооруженных конфликтах: учеб. пособие. М.: КНОРУС. 2017. 438 с.

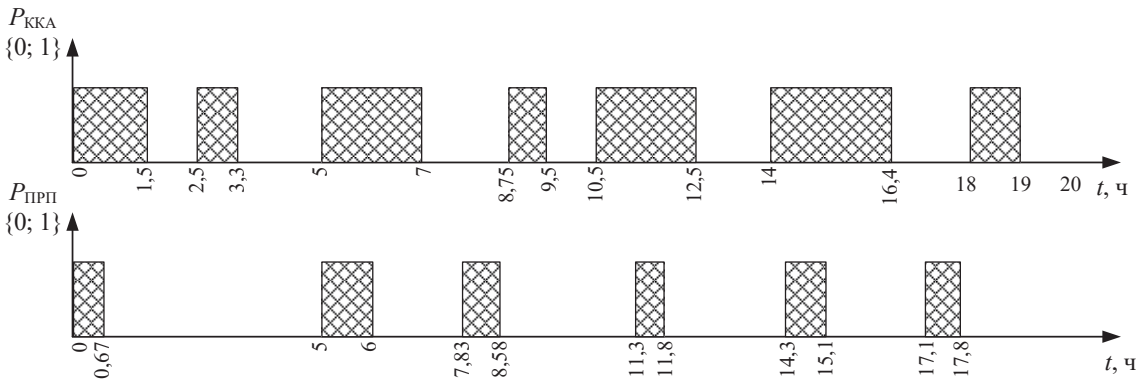

Рис. 6. Сценарий информационно-технического воздействия противоборствующей стороны

Таблица 1.

Исходные данные прогнозируемого сценария информационно-технического воздействия

Параметр	Численное значение (диапазон)	Физический смысл параметра, единица измерения
t_a t_b	0 20	Время начала и окончания рассматриваемого временного интервала соответственно, ч
$K_{\text{ст ИО тр}}$	0,8	Требуемое значение коэффициента стойкости информационного обмена
ПТВ в виде ККА		
$N_{\text{ККА}}$	7	Количество воздействий ККА
$t_{\text{н1}}$ $t_{\text{к1}}$	0 1,5	время начала и окончания 1-го воздействия ККА соответственно, ч
$t_{\text{н2}}$ $t_{\text{к2}}$	2,5 3,3	Время начала и окончания 2-го воздействия ККА соответственно, ч
$t_{\text{н3}}$ $t_{\text{к3}}$	5 7	Время начала и окончания 3-го воздействия ККА соответственно, ч
$t_{\text{н4}}$ $t_{\text{к4}}$	8,75 9,5	Время начала и окончания 4-го воздействия ККА соответственно, ч
$t_{\text{н5}}$ $t_{\text{к5}}$	10,5 12,5	Время начала и окончания 5-го воздействия ККА соответственно, ч
$t_{\text{н6}}$ $t_{\text{к6}}$	14 16,4	Время начала и окончания 6-го воздействия ККА соответственно, ч
$t_{\text{н7}}$ $t_{\text{к7}}$	18 19	Время начала и окончания 7-го воздействия ККА соответственно, ч
ЭВ в виде ПРП		
$N_{\text{ПРП}}$	7	Количество воздействий ПРП
$t_{\text{н1}}$ $t_{\text{к1}}$	0 0,67	Время начала и окончания 1-го воздействия ПРП соответственно, ч
$t_{\text{н2}}$ $t_{\text{к2}}$	5 6	Время начала и окончания 2-го воздействия ПРП соответственно, ч
$t_{\text{н3}}$ $t_{\text{к3}}$	7,83 8,58	Время начала и окончания 3-го воздействия ПРП соответственно, ч
$t_{\text{н4}}$ $t_{\text{к4}}$	11,3 11,8	Время начала и окончания 4-го воздействия ПРП соответственно, ч
$t_{\text{н5}}$ $t_{\text{к5}}$	14,3 15,1	Время начала и окончания 5-го воздействия ПРП соответственно, ч
$t_{\text{н6}}$ $t_{\text{к6}}$	17,1 17,8	Время начала и окончания 6-го воздействия ПРП соответственно, ч

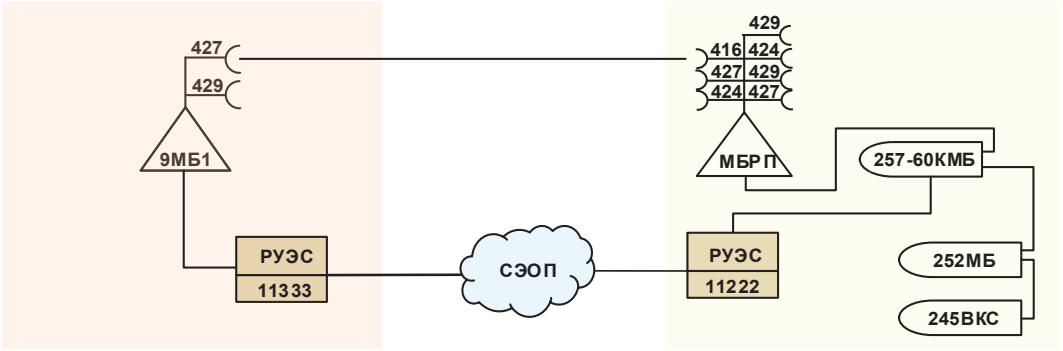

Рис. 7. Структура информационного направления ведомственной системы управления (вариант)

определить ВВХ свойства стойкости информационного обмена в ИН ведомственной СУ и оценить его показатели в условиях прогнозируемого сценария ИТВ (рис. 6) противоборствующей стороны.

Решение. В целях решения поставленной задачи разработана логико-вероятностная модель информационного обмена (рис. 8) в ИН ведомственной СУ заданной структуры (рис. 7). Указанная модель представлена совокупностью взаимосвязанных СФЦ исследуемого процесса в аппаратных (станциях) и районных узлах электросвязи (РУЭС) СЭОП, которые, в свою очередь, представлены базовыми моделями. Функциональные вершины 1, 2, 6, 11, 15, 17 отражают события прохождения информационного обмена без нарушения (блокирования) в аппаратных (станциях) и характеризуются функциями распределения вероятности времени стойкости к воздействию заданного сценария ИТВ. Вершины 4 и 8 отражают события прохождения информационного обмена без нарушения (блокирования) через РУЭС СЭОП.

Система логических уравнений для представленной модели информационного обмена в ИН имеет вид:

$$\begin{cases} y_1 = x_1;\ y_2 = x_2;\ y_3 = y_1; \\ y_4 = x_4;\ y_5 = y_2 \cdot y_4;\ y_6 = x_6; \\ y_7 = y_3 \cdot y_6;\ y_8 = x_8;\ y_9 = y_5 \cdot y_8; \\ y_{10} = y_7 + y_9;\ y11 = x_{11};\ y_{12} = y_{10} \cdot y_{11}; \\ y_{13} = y_{12} \cdot y_{14};\ y_{14} = y_{15};\ y_{15} = x_{15}; \\ y_{16} = y_{13} \cdot y_{17};\ y_{17} = x_{17}, \end{cases}$$

а вероятностная функция с учетом перехода от вероятностных мер к функциям распределения вероятности времени стойкости информационного обмена в аппаратных (станциях) и РУЭС СЭОП, описывается тремя одночленами:

$$F_{\text{ст ИО ИН}}(t) = F_{\text{ст ИО Р-409 МБ1}}(t)\ \text{РР} \times F_{\text{ст ИО Р-414 МБРП}}(t) \times$$
$$\times F_{\text{ст ИО П-257-60 КМБ}}(t) \times F_{\text{ст ИО П-252 МБ}}(t) \times F_{\text{ст ИО П-245 ВКС}}(t) +$$
$$+ F_{\text{ст ИО Р-409 МБ1 (КАС)}}(t)\ \text{Пр} \times F_{\text{ст ИО РУЭС}}(t) \times$$
$$\times F_{\text{ст ИО РУЭС}}(t) \times F_{\text{ст ИО П-257-60 КМБ}}(t) \times F_{\text{ст ИО П-252 МБ}}(t) \times$$
$$\times F_{\text{ст ИОП-245 ВКС}}(t) - F_{\text{ст ИОР-409 МБ1}}(t)\ \text{РР} \times$$
$$\times F_{\text{ст ИОР-409 МБ1(КАС)}}(t)\ \text{Пр} \times F_{\text{ст ИО РУЭС}}(t) \times$$

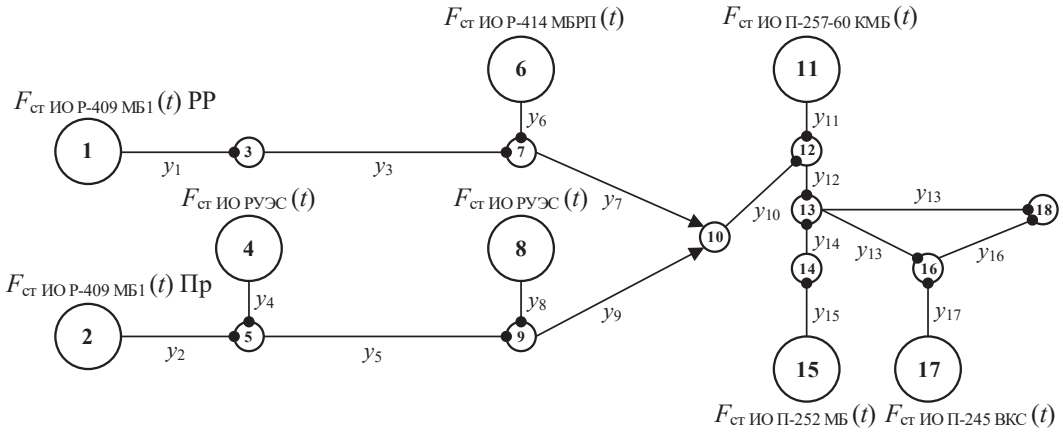

Рис. 8. Логико-вероятностная модель информационного обмена со свойством стойкости в информационном направлении ведомственной системы управления

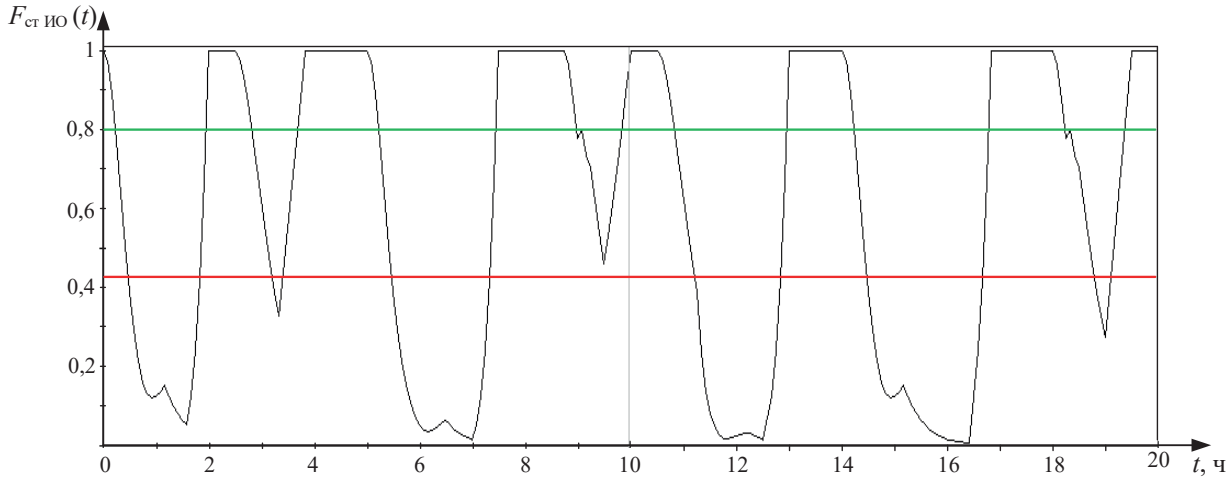

Рис. 9. График функции распределения вероятности времени стойкости информационного обмена в информационном направлении ведомственной системы управления

$$\times F_{\text{ст ИО РУЭС}}(t) \times F_{\text{ст ИО Р-414 МБРП}}(t) \times F_{\text{ст ИО П-257-60 КМБ}}(t) \times$$
$$\times F_{\text{ст ИОП-252 МБ}}(t) \times F_{\text{ст ИО П-245 ВКС}}(t)$$

С помощью программных комплексов автоматизированного структурно-логического моделирования ПК АСМ 2001.1 и Mathcad-2014 при заданных допущениях и ограничениях произведен расчет ВВХ свойства стойкости исследуемого процесса в ИН. График функции распределения вероятности времени стойкости информационного обмена в ИН ведомственной СУ представлен на рис. 9.

Численное значение оцениваемого показателя стойкости – коэффициента $K_{\text{ст ИО}}$ равно 0,418, что не соответствует требуемому ($K_{\text{ст ИО тр}} \geq 0{,}8$). Расчетные значения свидетельствует о том, что стойкость информационного обмена существенно снижена и не соответствует необходимой степени обеспечения управления, что объясняется стратегией комплексного согласованного применения противоборствующей стороной сил и средств ИТВ, а также отсутствием эффективных методов и средств защиты от ПТВ, в частности от СР, успешная реализация которой оказывает основное влияние на эффективность проведения ККА.

Полученный результат свидетельствует о необходимости проведения дальнейшего исследования по разработке организационно-технических мероприятий, направленных на защиту процесса обмена информацией, что позволит обеспечить безопасность информационного обмена в ведомственных СУ.

Выводы

Сущность полученного научного результата заключается в предложенной многоуровневой логико-вероятностной модели информационного обмена, которая позволила:

- выявить закономерности динамики прохождения информационного обмена в ведомственной СУ и оценить его стойкость в условиях воздействия комплекса ДФ ИТВ;
- использовать стратифицированный подход, который на основе базовой логико-вероятностной модели информационного обмена, позволяет создавать СФЦ исследуемого процесса любого уровня декомпозиции в СУ различной топологической структуры;
- учесть на различных уровнях декомпозиции информационного обмена модели исследуемого процесса любого из нижележащих уровней;
- учесть динамику информационного противоборства посредством задания временных параметров ДФ ИТВ.

Литература

1. Иванец В. М., Лукьянчик В. Н., Мельник В. Н. Особенности организации управления войсками в операции с учетом динамики информационных процессов при переходе на военные сетевые технологии // Военная мысль. 2020. № 7. С. 91–101.
2. Потапчик Н. Н. Методический подход к оценке стойкости информационного обмена в условиях информационно-технического воздействия противника // Вестник Военной академии Республики Беларусь. 2024. № 3(84). С. 36–50.
3. Шерстобитов Р. С. Модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки // Системы управления, связи и безопасности. 2025. № 1. С. 79–104.
4. Леонов Н. В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2(60). С. 81–92.
5. Пылинский М. В., Потапчик Н. Н. Организационно-технические требования к функционированию телекоммуникационных сетей группировки войск (сил) в условиях сетевых атак противника // Вестник Военной академии Республики Беларусь. 2024. № 1(82). С. 11–18.
6. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. СПб.: Наукоемкие технологии, 2020. 337 с.
7. Стародубцев Ю. И., Закалкин П. В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. № 4(62). С. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
8. Богер А. М., Соколов А. Н. Математическая модель вектора DDOS-атаки на сетевую инфраструктуру АСУ ТП с использованием метода топологического преобразования стохастических сетей // Вопросы кибербезопасности. 2023. № 4(56). С. 72–79.
9. Пылинский М. В., Потапчик Н. Н. Методический подход к оценке функционирования системы военной связи в условиях информационно-технического воздействия // Вестник Военной академии Республики Беларусь. 2023. № 1(78). С. 18–23.
10. Тишков В. В., Иванов В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. 2023. № 9. С. 59–72.

MULTILEVEL LOGICAL-PROBABILISTIC MODEL OF INFORMATION EXCHANGE IN DEPARTMENTAL MANAGEMENT SYSTEM

Potapchik N. N.[6], Pylinsky M. V.[7]

Keywords: *information warfare, telecommunications subsystem, information technology impact, destabilizing factor, information exchange security, property of stability, general logical-probabilistic method.*

Abstract

The purpose: *of the work: is to develop a multilevel logical-probabilistic model of information exchange with the property of stability in a departmental management system.*

Research method: *the conducted research is based on general scientific methods: analysis, synthesis, abstraction, generalization, modeling, induction, deduction. The general logical-probabilistic method, as well as probability theory, were justifiably chosen and used as the main method.*

Research results: *a multilevel logical-probabilistic model of information exchange with the property of stability has been developed, including private models of the process under study in vulnerable subsystems and elements of the telecommunications subsystem of the departmental control system. The presented model allows to obtain equations of probability functions of the property of stability of information exchange,*

6 Nikolay N. Potapchik, Adjunct of the Department of Communications, Faculty of Communications and Automated Control Systems, Military Academy of the Republic of Belarus, Minsk, Republic of Belarus. E mail: nikpotapchik89@gmail.com

7 Maxim V. Pylinsky, Dr.Sc. of Military Sciences, Professor, Head of the Department of Communications, Faculty of Communications and Automated Control Systems, Military Academy of the Republic of Belarus, Minsk, Republic of Belarus. E-mail: pylinskii.maksim@mail.ru

exposed to the influence of a complex of destabilizing factors of information-technical influence, to establish new quantitatively substantiated dependencies between input and output parameters and to evaluate stability of the studied process in the departmental management system. The adequacy of the developed model has been proven. In the main part of the article, using the presented model, the calculation and assessment of the probabilistic-temporal characteristics of the property of stability of information exchange in the information direction of the departmental management system is carried out. The results of the assessment indicate the need to develop organizational and technical measures aimed at ensuring the security of information exchange in departmental management systems.

Scientific novelty: *the presented multilevel logical-probabilistic model allows: to identify patterns of dynamics of information exchange in departmental control systems; to use a stratified approach, which, based on the basic logical-probabilistic model of information exchange, allows to create schemes of functional integrity of the studied process of any level of decomposition in control systems of different topological structure; to take into account the dynamics of information confrontation by setting time parameters of destabilizing factors of information-technical influence.*

References

1. Ivanec V. M., Luk'janchik V. N., Mel'nik V. N. Osobennosti organizacii upravlenija vojskami v operacii s uchetom dinamiki informacionnyh processov pri perehode na voennye setevye tehnologii // Voennaja mysl'. 2020. № 7. S. 91–101.
2. Potapchik N. N. Metodicheskij podhod k ocenke stojkosti informacionnogo obmena v uslovijah informacionno-tehnicheskogo vozdejstvija protivnika // Vestnik Voennoj akademii Respubliki Belarus'. 2024. № 3(84). S. 36–50.
3. Sherstobitov R. S. Model' maskirovanija informacionnyh napravlenij setej peredachi dannyh vedomstvennogo naznachenija v uslovijah komp'juternoj razvedki // Sistemy upravlenija, svjazi i bezopasnosti. 2025. № 1. S. 79–104.
4. Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 1. Ontologicheskaja model' // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 81–92.
5. Pylinskij M. V., Potapchik N. N. Organizacionno-tehnicheskie trebovanija k funkcionirovaniju telekommunikacionnyh setej gruppirovki vojsk (sil) v uslovijah setevyh atak protivnika // Vestnik Voennoj akademii Respubliki Belarus'. 2024. № 1(82). S. 11–18.
6. Makarenko S. I. Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. SPb.: Naukoemkie tehnologii, 2020. 337 s.
7. Starodubcev Ju. I., Zakalkin P. V. Strukturno-funkcional'nyj analiz konfliktnoj situacii mezhdu gosudarstvennoj sistemoj obespechenija informacionnoj bezopasnosti i inostrannoj sistemoj destruktivnyh vozdejstvij // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 82–91. DOI: 10.21681/2311-3456-2024-4-82-91.
8. Boger A. M., Sokolov A. N. Matematicheskaja model' vektora DDOS-ataki na setevuju infrastrukturu ASU TP s ispol'zovaniem metoda topologicheskogo preobrazovanija stohasticheskih setej // Voprosy kiberbezopasnosti. 2023. № 4(56). S. 72–79.
9. Pylinskij M. V., Potapchik N. N. Metodicheskij podhod k ocenke funkcionirovanija sistemy voennoj svjazi v uslovijah informacionno-tehnicheskogo vozdejstvija // Vestnik Voennoj akademii Respubliki Belarus'. 2023. № 1(78). S. 18–23.
10. Tishkov V. V., Ivanov V. G., Luk'janchik V. N. Obosnovanie oblika postroenija perspektivnyh kompleksov i sredstv svjazi na osnove opyta organizacii svjazi pri provedenii special'noj voennoj operacii // Voennaja mysl'. 2023. № 9. S. 59–72