Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 80 – 86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

МЕТОДИКА ПРОВЕДЕНИЯ ДИАГНОСТИРОВАНИЯ КИБЕРНЕТИЧЕСКОЙ СТОЙКОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

д.т.н., профессор Забара Станислав Сергеевич,
Институт компьютерных технологий Открытого международного университета развития человека «Украина», г. Киев, Украина
д.т.н., профессор Хлапонин Юрий Иванович,
Киевский национальный университет строительства и архитектуры, г. Киев, Украина
Козубцова Леся Михайловна,
Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина

АННОТАЦИЯ. В статье проанализированы известные попытки решений научной задачи расчета кибернетической стойкости информационной системы специального назначения. Установлено, что на данное время существующие решения не учитывают при расчете кибернетической стойкости активное действий деструктивных информационных влияний, а результат носит статический характер, который отображает состояние составных системы политике безопасности. Безусловно этого недостаточно для оценки реального состояния. В результате этого возникла необходимость в разработке методики диагностирования, которая бы обеспечивала расчет кибернетической стойкости информационной системы специального назначения по результатам активных кибернетических действий. Предложен математический аппарат методики обеспечивает расчет кибернетической стойкости информационной системы специального назначения для модели наихудшего варианта, для так называемого наступления события угрозы нулевого дня.

Практическое значение и применение заключается в практичной возможности определения уровня кибернетической стойкости информационной системы специального назначения с учетом активных действий деструктивных информационных влияний на стадии проектирования и эксплуатации системы.

Научная новизна. Научная новизна полученного результата заключается в том, что предложено решение научно-практической задачи расчета кибернетической стойкости информационной системы специального назначения с учетом активных действий деструктивных информационных влияний угрозы нулевого дня.

КЛЮЧЕВЫЕ СЛОВА: методика, оценка, кибернетическая стойкость, защищенность, надежность, живучесть, информационная система специального назначения, деструктивное информационное влияние.

METHODS FOR DIAGNOSING CYBERNETIC STABILITY OF A SPECIAL PURPOSE INFORMATION SYSTEM

doctor of technical Sciences, Professor Stanislav Zabara,
Institute of computer technologies of the Open international University of human development "Ukraine", Kiev, Ukraine
doctor of technical Sciences, Professor Yuri Khlaponin,
Kiev national University of construction and architecture, Kiev, Ukraine
Lesya Kozubtsova,
Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

ABSTRACT. The article analyzes well-known attempts to solve the scientific problem of calculating the cybernetic stability of a special-purpose information system. It is established that at this time, existing solutions do not take into account the active actions of destructive information influences when calculating cybernetic stability, and the result is static, which reflects the state of the components of the security policy

system. Of course, this is not enough to assess the real state. As a result, it became necessary to develop a diagnostic technique that would provide a calculation of the cybernetic stability of a special-purpose information system based on the results of active cybernetic actions. The mathematical apparatus of the method provides calculation of cybernetic stability of a special-purpose information system for the worst-case scenario model, for the so-called zero-day threat event.

The practical significance and application lies in the practical possibility of determining the level of cybernetic stability of a special-purpose information system, taking into account the active actions of destructive information influences at the stage of design and operation of the system.

Scientific novelty. The scientific novelty of the result is that a solution to the scientific and practical problem of calculating the cybernetic stability of a special-purpose information system is proposed, taking into account the active actions of destructive information influences of the zero-day threat.

KEYWORDS: methodology, assessment, cybernetic stability, security, reliability, survivability, special-purpose information system, destructive information influence.

ВВЕДЕНИЕ. Информационные системы (ИС) применяются для решения широкого спектра научных и производственных задач сбора, обработки, накопления и хранения информации, управления критическими объектами в реальном масштабе времени. Эти задачи имеют актуальное значение в повседневной деятельности специальных пользователей. Для таких пользователей, которые решают эти задачи, информационные системы начали именовать, как информационные системы специального назначения (ИС СН) (рис. 1).

Функционирование ИС СН в новой среде – киберпространстве, порождает новые уязвимости и угрозы. Отсюда высокий уровень требований, предъявляемых к надежности информационных систем [1 – 4]: адекватность, оптимальность, оперативность, устойчивость, непрерывность, скрытность (рис. 2). Из множества перечисленных свойств процесса управления в диссертационном исследовании ограничимся рассмотрением устойчивостью. И как следствие, необходимо разработать новый инструментарий обеспечения безопасности ИС, под которой понимается состояние ее защищенности, что обеспечивает устойчивое функционирование в условиях действий деструктивных информационных воздействий (ДИВ).

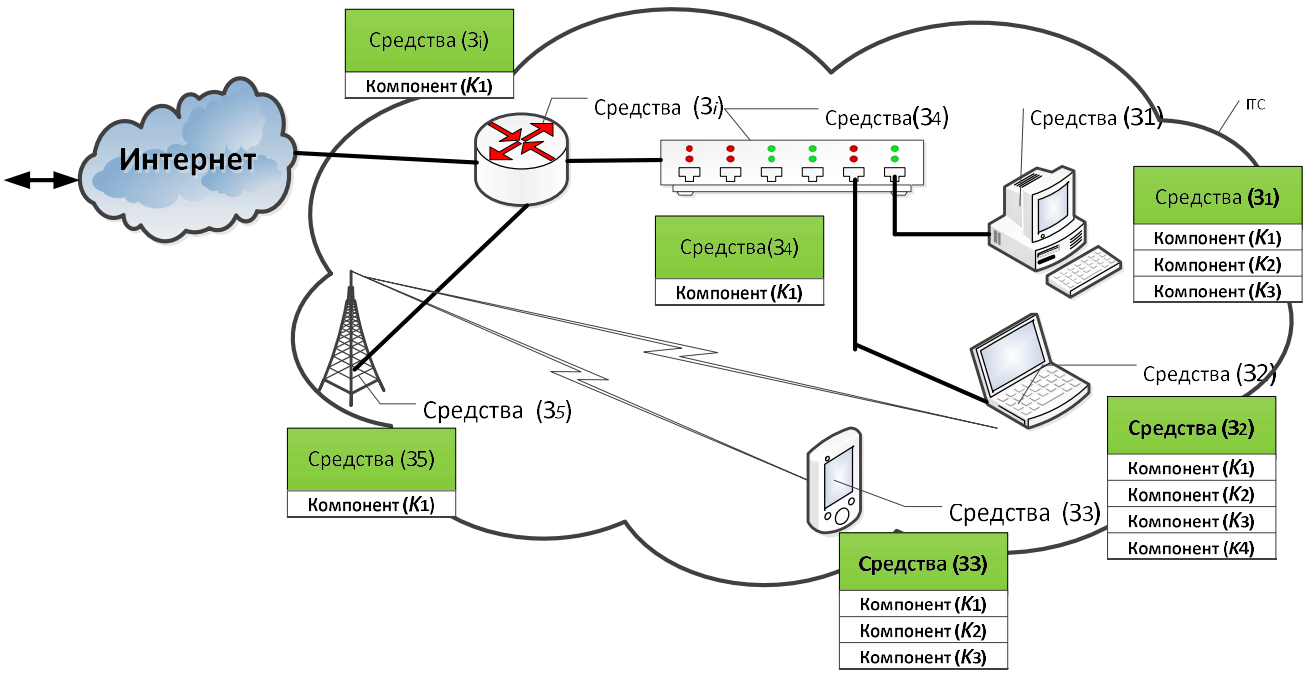

Рис. 1. Фрагмент информационной системы специального назначения

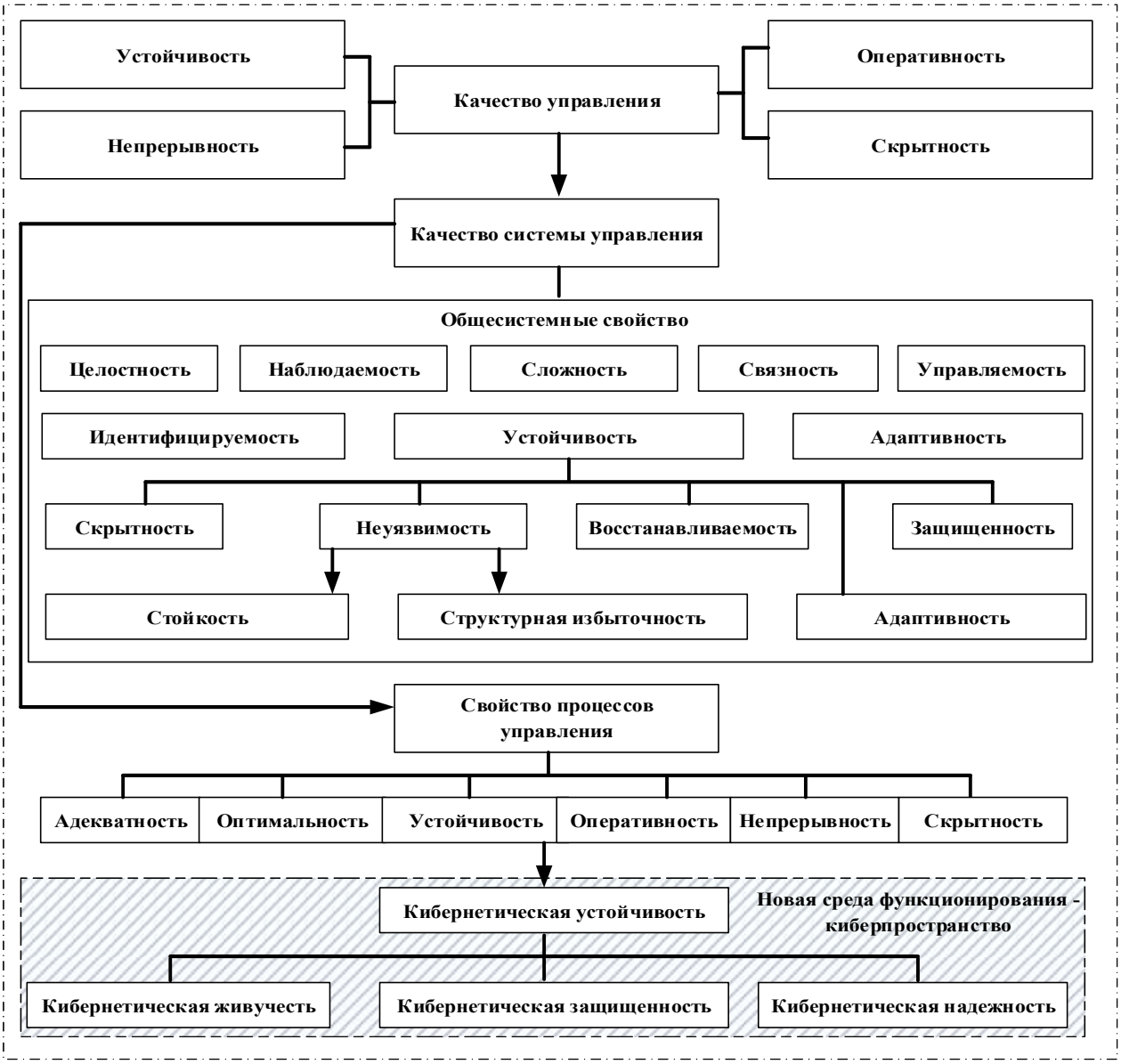

Рис. 2. Место понятия «кибернетическая устойчивость» в классификации

Согласно цели, объекта, предмета и определенного научного задания диссертационного исследования необходимо разработать методику диагностирования кибернетической устойчивости функционирования информационной системы специального назначения (ИС СН) в кибернетическом пространстве.

Анализ последних исследований и публикаций по данному направлению. Поиск в открытых источниках информации по ключевому слову «кибернетическая устойчивости ИС СН» дал возможность найти только понятие «кибернетическая устойчивости ИС», которое на первый взгляд тождественные «ИС СН», но это совсем не так.

В исследованиях [5 – 7] введено в употребление понятие киберустойчивости объекта критической информационной инфраструктуры (КИИ). В коллективной работе [8, с. 46] обосновано понятие «киберустойчивость объекта критической инфраструктуры (КИ).

В целом мы согласны с классификацией (рис. 2) предложенной в работах [5 – 8], тогда «кибернетическая устойчивость $P_{КС(S)}$ ИС СН» по классике состоит из следующих компонентов (1):

$$P_{КС(S)} = P_{КЖ(S)} \text{ x } P_{КН(S)} \text{ x } P_{КЗ(S)} \quad (1)$$

Где $P_{КЖ(S)}$ – кибернетическая живучесть, это вероятность сохранения ее работоспособности (выживания) в условиях выхода из строя технических средств обработки информации; $P_{КЗ(S)}$ – кибернетическая защищенность ИС СН, это вероятность обеспечения выполнения целевой функции ИС СН с заданным качеством в условиях применения «общих» и целенаправленных деструктивных информационных воздействий; $P_{КН(S)}$ – кибернетическая надежность ИС СН, это вероятность обеспечения выполнения целевой функции ИС СН на протяжении определенного временного интервала в условиях возникновения программных ошибок, технических сбоев и непреднамеренных ошибочных действий технического персонала и должностных лиц.

Цель статьи. Апробировать структуру методики диагностирования устойчивого функционирования кибернетической ИС СП в кибернетическом пространстве и зону ответственности участников эксперимента.

ОСНОВНОЙ РЕЗУЛЬТАТ

Методика диагностирования устойчивого функционирования кибернетической ИС СН в кибернетическом пространстве включает следующие этапы:

Этап 1. Реализация мероприятий по категорированию и декомпозиции ИС СН на средства и компоненты (элементы) относительно уязвимых к деструктивных информационных воздействий.

Этап 2. Выбор мер кибербезопасности для каждого средства и компоненты (элемента) составляющих ИС СН.

Этап 3. Процедуры по реализации мер кибербезопасности на каждом средстве и компоненте (элементы) составляющих ИС СН.

Этап 4. Диагностирование уровня достижения реализуемости процедур кибербезопасности на каждом средстве и компоненте (элементы) составляющих ИС СН в соответствии с мероприятий.

Этап 5. Расчет показателя устойчивости функционирования кибернетической ИС СН в кибернетическом пространстве. (**Методика расчета составляющих показателя кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве).**

Для наглядности единства разработанных уточняющих методик, которые позволяют рассчитать необходимые компоненты кибернетической устойчивости функционирования ИС СН по результатам диагностирования, представлено в виде блок-схемы (см. рис. 3).

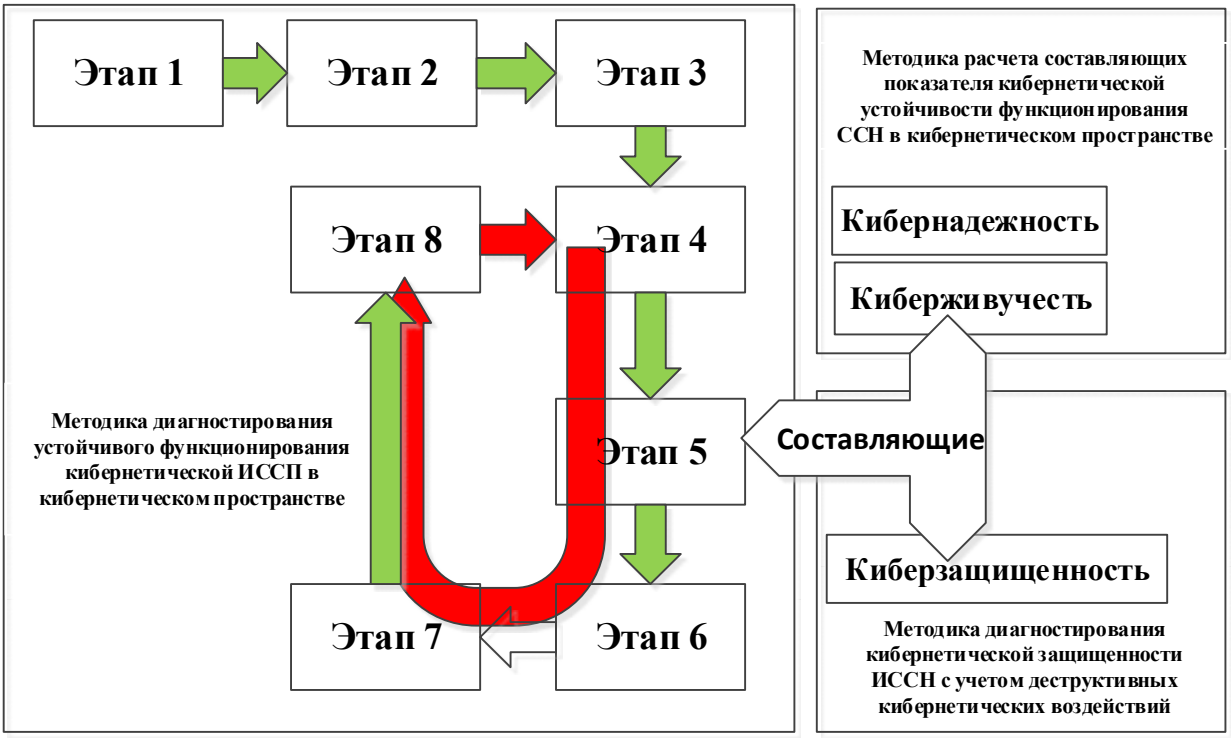

Рис. 3. Бока-схема методики диагностирования кибернетической устойчивого функционирования ИС СН в кибернетическом пространстве

Вычисление основывается на методике расчета составляющих показателя устойчивости функционирования кибернетической ИС СН в кибернетическом пространстве и в общем виде методика представлена следующими этапами:

Этап 5.1. Диагностирование и расчет кибернетической защищенности $P_{КЗ(S)}$ ИС СН [9; 10].

Этап 5.2. Расчет кибернетической надежности $P_{КН(S)}$ ИС СН.

Этап 5.3. Расчет кибернетической живучести $P_{КЖ(S)}$ ИС СН.

Этап 5.4. Расчет кибернетической устойчивости $P_{КС(S)}$ функционирования ИС СН.

Этап 6. Обработка, анализ и оценка результатов диагностирования кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве.

Этап 7. Отработка (представления) практических рекомендаций по дальнейшей безопасной эксплуатации ИС СН в кибернетическом пространстве.

Этап 8. Эпизодический (внезапный) мониторинг ИС СН в рамках этапов 4-7.

Методика апробирована в работе [11].

Методика расчета составляющих показателя кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве включает следующие этапы:

В общем виде методика расчета составляющих показателя кибернетической устойчивости представлена следующими этапами:

Этап 1. Сбор и анализ исходных данных необходимых для расчета кибернетической устойчивости функционирования ИС СН.

Этап 2 Расчет кибернетической устойчивости ($P_{КС(KjZi)}$) функционирования компонента (K_j), который есть составляющей средства (Z_i) ИС СН.

Этап 2.1 Диагностирование и расчет кибернетической защищенности ($P_{КЗ(KjZi)}$) компонента (K_j), который есть составляющей средства (Z_i) ИС СН в соответствии [9; 10].

Этап 2.2 Расчет надежности кибернетической ($P_{КН(KjZi)}$) компонента (K_j), которая есть составляющей средства (Z_i) ИС СН.

Этап 2.3 Расчет кибернетической живучести **(**$P_{КН(KjZi)}$**)** компонента (K_j), которая есть составляющей средства (Z_i) ИС СН. Этап 2.4 Расчет кибернетической устойчивости ($P_{КС(KjZi)}$) функционирования компоненты (K_j) со склада средства (Z_i) ИС СН.

Этап 3 Расчет кибернетической устойчивости ($P_{КС(Zi)}$) функционирования средств (Z_i) ИС СН.

Этап 3.1 Диагностирование и расчет кибернетической защищенности ($P_{КЗ(Zi)}$) каждого средства (Z_i) ИС СН рассчитывается в соответствии [9; 10].

Этап 3.2 Расчет кибернетической надежности ($P_{КН(Zi)}$) каждого средства (Z_i) ИС СН.

Этап 3.3 Расчет кибернетической живучести ($P_{КЖ(Zi)}$) в пределы состояний каждого средства (Z_i) ИС СН.

Этап 3.4 Расчет кибернетической устойчивости ($P_{КС(Zi)}$) функционирования средства (Z_i) ИС СН.

Этап 4 Расчет кибернетической устойчивости ($P_{КС(S)}$) функционирования ИС СН.

Этап 4.1 Расчет кибернетической защищенности ($P_{КЗ(S)}$) ИС СН в целом рассчитывается в соответствии [9; 10].

Этап 4.2 Расчет кибернетической надежности **(**$P_{КН(S)}$) ИС СН в целом.

Этап 4.3 Расчет кибернетической живучести ($P_{КЖ(S)}$) ИС СН в целом.

Этап 4.4 Расчет кибернетической устойчивости ($P_{КС(S)}$) ИС СН в целом.

Этап 5. Обработка, анализ и оценка результатов диагностирования кибернетической устойчивости функционирования ИС СН в кибернетическом пространстве. Формализация результатов.

Методика подготовлена и проходит предварительную апробацию, поэтому является предметом дальнейшее публикации.

Методика диагностирования кибернетической защищенности информационной системы с учетом деструктивных кибернетических воздействий включает следующие этапы:

Этап 1. Реализация мероприятий по категоризации и разложения ИС СН на компоненты и элементы уязвимости кибернетического воздействия

Этап 2. Расчет показателей $P_{КЗ(KjZi)}$ кибернетической защищенности каждого компонента (K_j),

который есть составляющей средства (Z_i) ИС СН.

Этап 3. Вычисления показателя $P_{КЗ(Zi)}$ каждого средства (Z_i) со склада ИС СН.

Этап 4. Расчет $P_{КЗ(S)}$ кибернетической защищенности ИС СН в целом.

Этап 5. Обработка, анализ и оценка результатов испытаний.

Методика многократно апробирована, а именно при оценке кибернетической защищенности системы связи организации [9] и информационно-телекоммуникационной системы [10].

Особенности практической реализации обобщенной методики.

1 Состав группы экспериментального диагностирования кибернетической устойчивого функционирования ИС СП в кибернетическом пространстве

1) Руководитель комиссии группы специалистов с кибербезопасности.

2) группы специалистов с кибербезопасности по направлениям и ответственности:

группа №1 фиксирования изменений состояния функционирования ИС СН;

группа №2 кибернетического влияния на ИС СН – отработки кибернетических действий в роли «хакера»;

группа №3 математического расчету кибернетической стойкости ИС СН – рассчитывают все параметры на всех этапах испытаний;

группа №4 условны пользователи (АРМ) ИС СН – осуществляют фиксирование передачи голосовых, текстовых, графических данных, потока видеоданных.

Порядок взаимодействия участников испытаний по данной методике:

специалисты контроля и фиксирования непосредственно с группой расчета;

руководитель испытаний через команду осуществления кибернетического влияния с условным хакером.

Запрещается лицам, которые осуществляют кибернетическое влияние (№2) сообщать начало наступления события кибернетического влияния группе №1.

ВЫВОДЫ.

Важнейшими научными и практическими результатами являются:

1. Усовершенствована методика диагностирования кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве. Методика основывается на введении отдельного этапа вычисления кибернетической устойчивости функционирования информационной системы специального назначения. В предложенной методике, в отличие от известных, предложена декомпозиция ИС СН на отдельные средства и компоненты по критериям конфиденциальности, целостности и доступности. Это позволило обеспечить более качественный отбор компонентов информационной системы специального назначения по критерию уязвимости деструктивным информационным воздействием.

2. Усовершенствована методика расчета составляющих показателя кибернетической устойчивости функционирования информационной системы специального назначения в кибернетическом пространстве. Методика основывается на расширении свойств кибернетической устойчивости, что является интегральным показателем кибернетической защищенности, надежности и живучести. Необходимость введения нового свойства вызванная новой средой функционирования информационной системы специального назначения в киберпространстве. Применение нового типа оружия – кибернетического оружия создает деструктивные информационные воздействий, которые нарушают нормальное функционирование системы.

3. Усовершенствована методика диагностирование кибернетической защищенности информационной системы специального назначения. В предложенной методике, в отличие от известных, предложено рассчитать оценку кибернетической защищенности информационной системы специального назначения на некоторый момент времени $t_{ДИВ}$, в который осуществляется активное деструктивное информационное влияние на эту систему $F_{ДИВ} = 1$ с целью прогнозирования и предотвращения потерять некоторых актив (Ак). Математический аппарат методики обеспечивает расчет кибернетической защищенности информационной системы специального назначения для модели наихудшего варианта наступления события угрозы нулевого дня.

СПИСОК ЛИТЕРАТУРЫ

[1] Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 296 с.
[2] БоговикА.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.
[3] Давыдов А.Е., Савицкий О.К., Максимов Р.В. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. Москва: Воентелеком, 2015. 520 с.
[4] Шолудько В.Г., Єсаулов М.Ю., Вакуленко О.В., Гурський Т.Г., Фомін М.М. Організація військового зв'язку : навчальний посібник. К.: ВІТІ, 2017. 282 с.
[5] Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. №2. С. 52 – 61.
[6] Минаев В.А., Крупенин А.В., Королев И.Д., Бондарь К.М., Захарченко Р.И. Оценка устойчивости функционирования критической информационной инфраструктуры // «Вестник РосНОУ», серия «Сложные системы: модели, анализ и управление». 2018. Вып. 4. Информатика и вычислительная техника. С. 129 – 138.
[7] Критическая информационная инфраструктура: оценка устойчивости функционирования / В.А. Минаев, И.Д. Королев, Е.В. Зеленцова, Р.И. Захарченко // Радиопромышленность, 2018. Т. 28. №4. С. 59 – 67.
[8] Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал «Електронне моделювання», 2019. Т.41. №1. С. 43 – 54.
[9] Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П Методика оцінки кібернетичної захищеності системи зв'язку організації // Сучасні інформаційні технології у сфері безпеки та оборони. 2018. №1(31). С. 43 – 46.
[10] Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П., Куцаєв В.В. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку // Збірник наукових праць ВІТІ. К.: ВІТІ, 2018. №2. С. 67 – 76.
[11] Козубцова Л.М. Апробація структури методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі // Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (17 березня 2020 року, м. Харків). Харків. Національна академія Національної гвардії України, 2020. С141 – 142.