УДК 004.056:004.738.5

С.П. Евсеев,
кандидат технических наук, доцент,
Ю.Е. Хохлачева,
кандидат технических наук,
О.Г. Король,
кандидат технических наук, доцент

ОЦЕНКА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ В ОРГАНИЗАЦИЯХ БАНКОВСКОГО СЕКТОРА НА ОСНОВЕ СИНЕРГЕТИЧЕСКОГО ПОДХОДА[1]

Исследована задача обеспечения непрерывности бизнес-процессов в организациях банковского сектора (ОБС) в условиях увеличения киберугроз для иерархической структуры критической инфраструктуры метасистемы государства.

Выделены основные стратегии и показатели оценки обеспечения непрерывности бизнес-процессов ОБС. Проанализировано влияние выбранных стратегий и решений по обеспечению непрерывности бизнеса на значения показателей непрерывности.

Ключевые слова: *кибертерроризм, кибератака, критическая инфраструктура, непрерывность бизнес-процессов.*

Досліджено завдання забезпечення безперервності бізнес-процесів в організаціях банківського сектора (ОБС) в умовах збільшення кіберзагроз для ієрархічної структури критичної інфраструктури метасистеми держави.

Виділено основні стратегії й показники оцінки забезпечення безперервності бізнес-процесів ОБС. Проаналізовано вплив обраних стратегій і рішень щодо забезпечення безперервності бізнесу на значення показників безперервності.

Ключові слова: *кібертероризм, кібератака, критична інфраструктура, безперервність бізнес-процесів.*

The issue of ensuring continuity of business processes in the organizations of the banking sector (OBS) in the conditions of increase in cyberthreats for hierarchical structure of critical infrastructure of metasystem of the state is investigated.

The main strategy and indicators of an assessment of ensuring continuity of business processes of OBS are allocated. Influence of the chosen strategy and decisions on ensuring continuity of business on values of indicators of continuity is analyzed.

Keywords: *cyberterrorism, cyber attack, critical infrastructure, continuity of business processes.*

Введение и анализ литературы

Изменение вектора безопасности мировых лидеров развитых стран в сторону обеспечения кибербезопасности объектов с критичной кибернетической структу-

[1] Закінчення. Початок у попередньому номері.

рой (ОККС), принятие стратегий и концепций с кибербезопасности ведущими мировыми государствами, создание национальных Команд реагирования на компьютерные инциденты (*Computer Emergency Response Team, CERT)* существенно изменило в последние десятилетия взгляды ведущих стран мира на становление феномена кибернетической безопасности и показывает, что толкование данной категории постоянно эволюционирует. На процесс эволюции взглядов существенно влияют уровень экономического развития страны, уровень образованности ее населения, степень внедрения высоких технологий, доступность к сети Интернет и т.п. Проведенный анализ основных принципов и методов реализации киберугроз в первой части статьи, позволяет сделать вывод, что в ближайшие один-два года резко возрастет количество и "качество" киберугроз на ОККС государства, позволяющих подорвать изнутри экономический базис государственной метасистемы [1; 2]. В этой связи вопросы, связанные с обеспечением непрерывности процессов управления в системах ОККС, являются первоочередными.

Целью работы является разработка структуры критической инфраструктуры метасистемы государства, рассмотрение задачи обеспечения непрерывности управления системы ОККС на примере непрерывности бизнес-процессов в организациях банковского сектора (ОБС) в условиях увеличения и масштабирования киберугроз.

Системы с критичной кибернетической структурой

Проведенный анализ основных положений систем с критичной кибернетической структурой в работе [1] позволяет использовать предложенные авторами основные понятия, связанные с формированием иерархической структуры критической инфраструктуры метасистемы государства:

Критическая инфраструктура (КИ) – системы, сети и/или отдельные объекты, целенаправленный или случайный вывод из строя которых может потенциально привести к непоправимым последствиям стабильного развития экономики и политических процессов в государстве, социального благополучия и здоровья населения.

Система с критичной кибернетической инфраструктурой (СККИ) – совокупность взаимосвязанных элементов, объединенных в единое целое, правильность функционирования и взаимодействия которых значительно влияет на кибернетическую безопасность государства на протяжении определенного интервала времени.

Объект с критичной кибернетической инфраструктурой (ОККИ) – элемент СККИ, кибернетическое влияние на которого приводит к снижению уровня его кибернетической защиты от киберугроз.

В табл. 1 приведены сравнительные результаты соотношения секторов государства к КИ [1].

Проведенный анализ табл.1 показал, что большинство развитых государств мира к наиболее уязвимым критическим инфраструктурам относят объекты, принадлежащие банковскому и финансовому сектору (сфере), энергетике и телекоммуникации.

Таблица 1

Сравнительная таблица критических инфраструктур

ГОСУДАРСТВО / СЕКТОР КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ	Большая Восьмерка															
	США	Япония	Германия	Великобритания	Франция	Италия	Канада	Российская федерация	Австралия	Австрия	Нидерланды	Новая Зеландия	Норвегия	Польша	Финляндия	Швеция
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Банки и финансы	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Водоснабжения	■	■	■	■	■	■	■		■	■	■		■	■	■	
Дамбы	■															
Энергетика	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Коммунальные сети			■						■	■			■		■	
Национальные символы	■						■			■						
Опасные материалы (Х, Б, Р, Я)	■	■		■			■							■		
Оборонно-промышленный комплекс	■	■			■		■	■	■						■	
Органы исполнительной власти	■		■	■			■		■		■	■	■	■		■
Органы судебной власти	■															
Охрана здоровья	■	■	■	■	■	■	■		■	■	■		■	■		■
Топливно-энергетический комплекс	■	■	■	■	■	■	■	■	■		■	■	■	■		
Почтовые службы	■									■						
Сельское хозяйство	■	■	■	■			■		■		■			■	■	
Система управления воздушным движением																■
Службы охраны общественного движения				■	■	■	■	■	■	■	■		■			
Службы экстренной помощи и реагирования на ЧС	■	■	■	■		■	■		■	■		■	■			
Телекоммуникации	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Транспорт	■	■		■	■	■	■	■	■	■	■	■	■	■	■	
Управления отходами		■		■		■	■		■				■			

На основе признакового подхода, предложенного в работе [1], предлагается иерархическая структура критической инфраструктуры метасистемы государства.

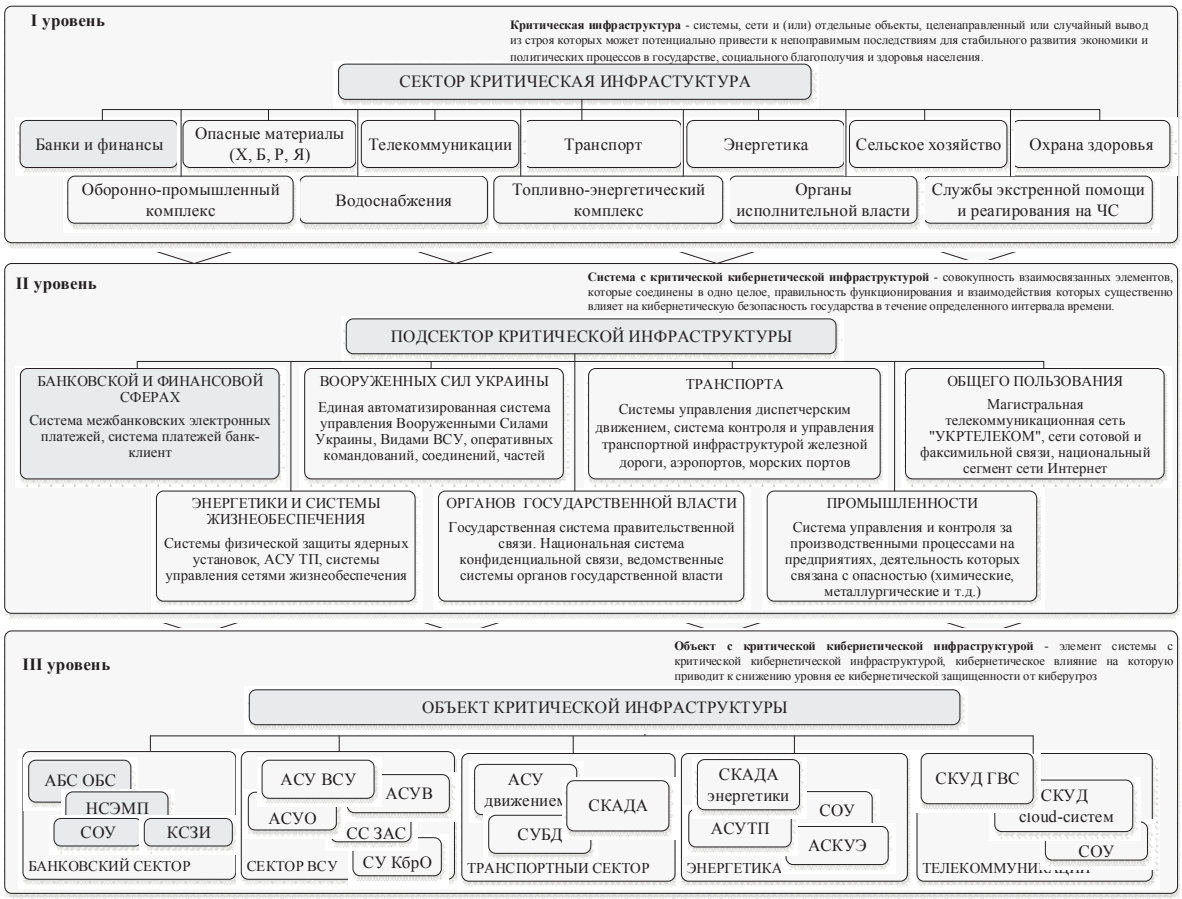

Рис. 1. Иерархическая структура критической инфраструктуры метасистемы государства

При этом под *метасистемой критичной инфраструктуры государства (МКИГ)* подразумивается система стратегического масштаба, представляющая собой совокупность значительного количества разнообразных элементов, объединенных в рамках единой критической кибернетической архитектуры в единую систему, обладающую синергизмом, и имеющую общее эмерджентное свойство (предназначение, функцию), отличающуюся от свойств отдельных элементов всей совокупности [1].

Стратегии и показатели обеспечения непрерывности бизнес-бизнеса в АБС ОБС. В любой социальной сфере (к которой относится и область обеспечения безопасности БИн в АБС ОБС) инциденты безопасности, прерывания работы (*disruptive events*) и аварии (*disasters*) неизбежны.

Однако их воздействие на деятельность компании должно быть минимизировано: данные должны быть сохранены, технические средства находится в рабочем состоянии, репутация спасена, люди − вне опасности [3, 4]. Решения указанных задач возможно осуществить в рамках управления непрерывностью бизнеса (*Business Continuity Management*) − целостного процесса управления, в рамках которого идентифицируются потенциальные угрозы деятельности организации, оцениваются возможные воздействия на бизнес-операции в случае реализации этих угроз, а также создается система предписаний для обеспечения способности организации восстанавливать свою деятельность и эффективно реагировать на инциденты, что позволяет гарантировать соблюдение интересов заинтересованных

сторон, обеспечить защиту репутации, бренда и создающих ценность операций. В первую очередь, при реализации стратегии и цикла управления непрерывностью необходимо обеспечить решение следующих задач [6].

Существует два основных инструмента непрерывности бизнес-процессов:

– план непрерывности бизнеса (*Business Continuity Planning*, BCP) – набор превентивных мер, детальных инструкций для действий в острых (критических) ситуациях, в ОБС дополнительно рассматриваются мероприятия по восстановлению БИн (восстановление данных БИн предполагает полную ясность в том, когда они были скопированы, что отражают, каков их формат, как их следует интерпретировать и прочее; определяется максимальный "возраст" данных, утрата которых допустима (*Recovery Point Objective*, RPO);

– планирование аварийного восстановления (*Disaster Recovery Planning*, DRP) – подготовка организации к скорейшему полному восстановлению ее деятельности в случае аварии, ЧП, бедствия, кризисной ситуации и т.п. [3–6].

Несмотря на различие, BCP и DRP являются неотъемлемыми частями менеджмента непрерывности бизнеса и процедурно пересекаются. В этом плане удобно их рассмотреть с помощью модели менеджмента PDCA (*Plan-Do-Check-Act*), основные задачи на этапах модели менеджмента PDCA представлены на рис. 2 [3; 7; 8].

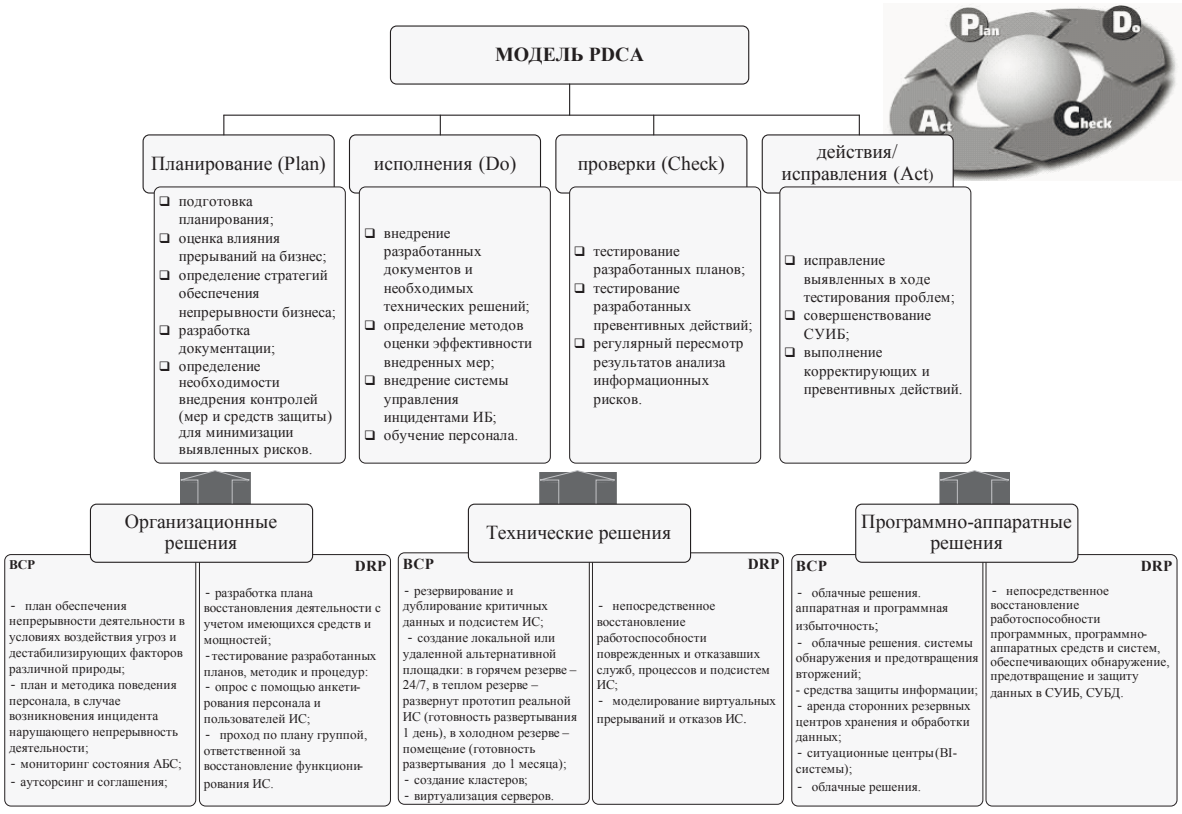

Рис. 2. Основные задачи и решения обеспечения непрерывности на этапах модели менеджмента PDCA

Таким образом, предлагаемые решения имеют свою стоимость, совместимость, сложность реализации, время развертывания и эффективность, и могут применяться как по отдельности, так и в виде комплекса мер, реализуемых до,

вовремя и/или после инцидента, вызвавшего нарушения непрерывности функционирования АБС и деятельности ОБС.

Оценка влияния прерываний на бизнес (*Business Impact Analysis*, BIA) является ключевой темой непрерывности бизнеса и состоит в функциональном анализе того, как прерывания повлияют на деятельность организации.

К задачам *BIA* относят:

определение ценности каждого бизнес-процесса;

идентификацию и ранжирование прерываний каждого бизнес-процесса;

приоритизацию бизнес-процессов;

оценку ресурсов на обеспечение непрерывности бизнес-процессов [3–6].

Итоговым результатом *BIA* является выбор стратегий управления непрерывностью бизнеса.

При определении ценности бизнес-процессов для информационных систем (АБС) могут быть зафиксированы значения ряда технических показателей, связь между которыми представлена на рис. 3:

MTPD (Maximum Tolerable Period of Disruption, максимально приемлемый период прерывания бизнеса) – период времени, по истечении которого неблагоприятные последствия, возникшие в результате прерывания бизнеса, становятся неприемлемыми;

RTO (Recovery Time Objective, целевое время восстановления) – период времени после произошедшего прерывания, в течение которого должен быть восстановлен минимальный уровень деятельности организации, а также поддерживающие его системы, прикладные программы и функции; полагается, что: *RTO* < *MTPD* [3–6].

RPO (Recovery Point Objective, целевая точка восстановления) – период времени, за которое должны быть восстановлены данные после прошедшего прерывания.

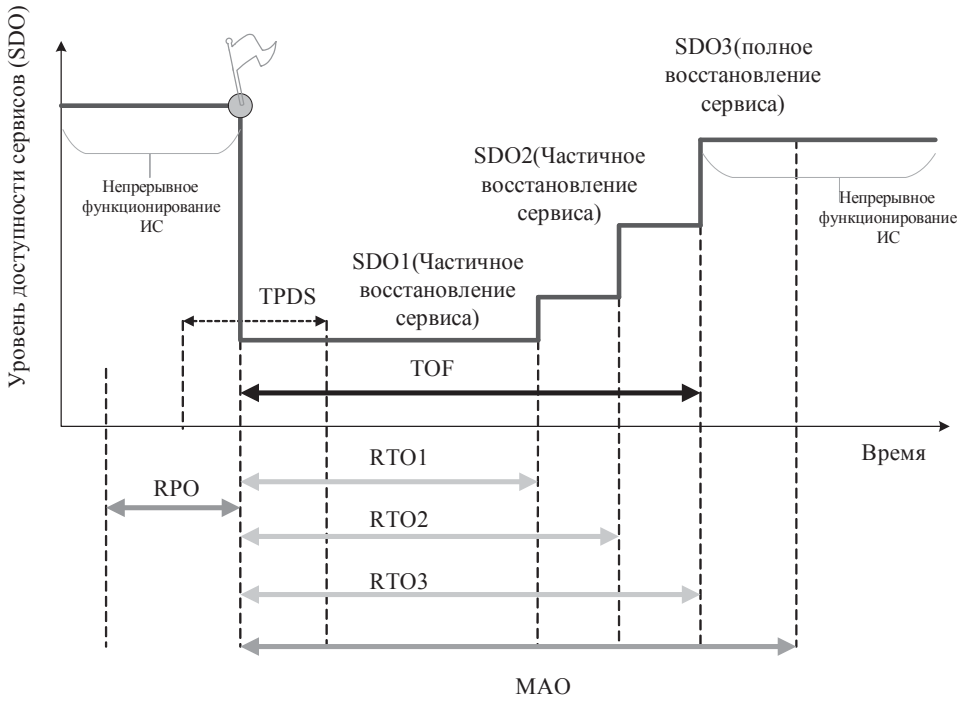

Рис. 3. Определение показателей непрерывности деятельности

MAO (Maximum Allowable Outage, максимально допустимое время простоя) – период времени, по истечении которого существует риск окончательного прекращения деятельности ОБС, в случае, если предоставление сервисов, данных, бизнес-процессов и/или услуг не будут возобновлены.

TOF (текущее время простоя) – период времени, в течение которого деятельность была прервана в результате отказа ИС или ее компонентов, недоступности сервисов и данных, в приемлемом для предприятия случае должна быть меньше максимально допустимого времени простоя. Полагается, что *TOFd"MAO*;

SDO (Service Delivery Objective, целевая доступность сервиса) – показывает уровень доступности сервиса в определенный момент времени;

TPDS – время планирования и развертывание решений обеспечения и восстановления непрерывности деятельности, в идеальном случае решения и планы должны быть разработаны и внедрены до наступления инцидента нарушения непрерывности, *TPDS << RTO*.

Анализ рис. 3 показал, что для снижения *TOF* необходим комплексный подход к решению задач BCP и DRP. Внедрение превентивных мер защиты от киберугроз, направленных на нарушение непрерывности, позволит не только минимизировать потери данных БИн в АБС, но и сократить целевое время восстановления данных.

Подобный эффект достигается за счет того, что планы и средства обеспечения непрерывности деятельности разрабатываются и развёртываются не во время отказа, а в период штатного функционирования АБС до реализации угрозы и возникновения лавинного эффекта. Это позволяет сразу после наступления инцидента скоординировать действия персонала и начать восстановление или полностью избежать простоя и потерь за счет оперативного переключения на резервную площадку (см. рис. 4) [5].

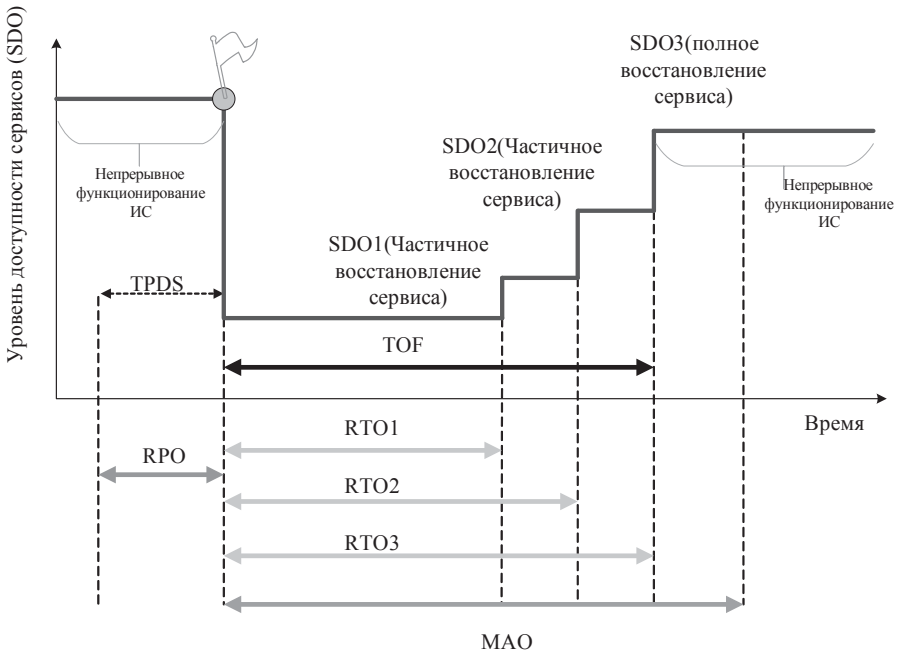

Рис. 4. Снижение времени восстановления функционирования АБС (TOF) за счет применения превентивных планов и мер защиты

Таким образом, для обеспечения комплексного подхода непрерывности бизнес-процессов ОБС предлагается использовать дублирование АБС на основе концепции альтернативных площадок (площадка в горячем резерве (*Hot Site*), площадка в теплом резерве (*Warm Site*), площадка в холодном резерве (*Cold Side*) с использованием стратегий актуализации данных – копирование резервных данных (*electronic vaulting*, *off-site data protection*, периодическая передача копий баз данных на альтернативные носители, обычно в пакетном режиме), удаленное журналирование (*remote journaling*, периодическая передача журнала выполненных транзакций с основной площадки на альтернативную), удаленное зеркалирование (*remote mirroring*, полное дублирование в реальном времени), что обеспечит требуемые показатели ценности бизнес-процессов.

Выводы

Таким образом, на основе проведенного анализа секторов (сфер) с СККИ предложена иерархическая структура критической инфраструктуры метасистемы государства, на ее основе рассмотрены основные задачи обеспечения непрерывности бизнес-процессов с учетом модели риска менеджмента PDCA, показатели оценки обеспечения непрерывности бизнес-процессов ОБС. Проанализировано влияние выбранных стратегий и решений по обеспечению непрерывности бизнес-процессов ОБС.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Грищук Р.В.* Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. *Леоненко Г.П.* Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины / Г.П. Леоненко, А.Ю. Юдин // Information Technology and Security". – 2013. – № 1(3). – С. 44–48.

3. *Дорофеев А.В.* Планирование обеспечения непрерывности бизнеса и восстановления / А.В. Дорофеев, А.С. Марков // Вопросы кибербезопасности. – 2015. – № 3(11). – С. 68–73.

4. *Барабанов А.В.* Семь безопасных информационных технологий / А.В. Барабанов, А.В. Дорофеев, А.С. Марков, В.Л. Цирлов ; под. ред. А.С. Маркова. – М. : ДМК Пресс, 2017. – 224 с.

5. *Оладько В.С.* Стратегии и показатели обеспечения непрерывности бизнеса / В.С. Оладько, С.Ю. Микова // Международный научный журнал // 2016. – № 7 Технические науки. – С. 109–112.

6. *Башнин А.* Ситуативное управление и непрерывность бизнеса. Ситуационные центры. ч. 3 / А. Башнин [Электронный ресурс]. – Режим доступа : http://upr.ru/article/kontseptsii-i-metody-upravleniya/.

7. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity [Электронный ресурс]. – Режим доступа : http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.

8. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements [Электронный ресурс]. – Режим доступа : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

Отримано 16.06.2017

Рецензент Хорошко В.О., д.т.н., проф.