© Dudatyev A. Method for complex information security management // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 2, p. 207-212.

МЕТОД УПРАВЛЕНИЯ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Андрей Дудатьев

Винницкий национальный технический университет, Украина

ДУДАТЬЕВ Андрей Вениаминович, к.т.н.

Год и место рождения: 1960 год, г. Кривой Рог, Днепропетровская область, Украина.
Образование: Винницкий политехнический институт, 1984 год.
Должность: докторант, доцент кафедры защиты информации ВНТУ.
Научные интересы: информационная безопасность социотехнических систем, модели и методы информационных войн, безопасность критических инфраструктур.
Публикации: более 60 научных работ, среди которых научные статьи, патенты и учебные пособия.
E-mail: andreysaf60@mail.ru

Аннотация. *Функционирование любого современного объекта, деятельность которого связана с предоставлением услуг или производством различной продукции, связана с решением актуальной задачи – обеспечением комплексной информационной безопасности. При этом под обеспечением комплексной информационной безопасности понимаем решение двух задач: обеспечение информационной безопасности или защита собственных информационных ресурсов и защита от возможных информационно-психологических воздействий конкурентов. В предложенной статье возможные нарушения информационной безопасности рассмотрены как потенциально возможные конфликтные ситуации, которые могут возникнуть на разных уровнях управления и сопровождаться различного рода противоборствами как элементами гибридной войны за ресурсы. Приведена теорема, формализующая необходимые и достаточные условия эффективного функционирования современного предприятия как объекта комплексной защиты. В статье впервые введено понятие информационной обфускации как технологии запутывания человека во время проведения специальных информационно-психологических воздействий и предложен универсальный и гибкий метод управления комплексной информационной безопасностью, который учитывает специфику этапов жизнедеятельности, как объекта защиты, так и комплексной системы защиты информации. Предложенный метод предлагается интегрировать в структурах ситуационных центров, что позволит обеспечить необходимый уровень защищённости данного объекта на уровне «предприятие-регион-государство».*

Ключевые слова: *комплексная информационная безопасность, метод управления комплексной информационной безопасностью, информационная война, информационно-психологическая операция, информационная обфускация, комплексная система защиты информации.*

Введение

Подход к совершенствованию функционирования любого предприятия, достижения цели его работы, которая в большинстве случаев сводится к занятию лидерства на определённом сегменте рынка, сводится к повышению эффективности всех производственных процессов. Современные информационные системы и информационные технологии играют одну из ведущих ролей в решении задач повышения эффективности всех производственных процессов в целом. Обеспечение безопасности информационной системы, непосредственно информационных ресурсов предприятия, а также всех остальных ресурсов является одной из приоритетных задач для современного предприятия. Существование конкурентной информационной среды, т.е. среды в которой проводятся специальные информационно-психологические операции со стороны потенциальных конкурентов, целью которых является минимизация влияния или уничтожение своих оппонентов, говорит о необходимости организации комплексной защиты. При этом под комплексной защитой подразумевается решение двоединой задачи: защиты собственных информационных ресурсов и защите от негативного информационного влияния конкурентов.

Анализ существующих исследований

Результаты исследования проблемы оценки и обеспечения или управления информационной безопасностью представлены во многих зарубежных [1] и отечественных источниках [2]. В приведённых работах представлены методы оценки рисков, связанных с информационными угрозами и управлением информационной безопасностью на разных уровнях детализации сложных систем. Однако, отсутствуют работы, где проблема комплексной информационной безопасности исследуется с точки зрения необходимости одновременной защиты информационных ресурсов

в условиях ведения информационной войны, т.е. ведения специальных информационно-психологических операций (ИПО), которые одновременно могут проводиться против технической и социальной составляющей социотехнических систем (СТС), к которым относятся и предприятия. Нерешённой проблемой остаётся задача алгоритмизации процесса начала и окончания информационной войны. Это также накладывает определённые трудности при построении эффективной защиты от негативных информационно-психологических воздействий. В практической плоскости эта проблема для защиты от негативного влияния может быть реализована путём смены, например, операций информационно-психологического воздействия на человека, как элемента СТС. Функционально это сопоставимо с программной обфускацией и может быть определено как *информационная обфускация*, т.е. применение технологий запутывания человека в процессе восприятия и анализа получаемой информации. При этом, конечно же, представляемая информация должна полностью сохранять свою функциональность. Таким образом, главной задачей *информационной обфускации* является создание алгоритма применения различных информационно-психологических операций для представления информации в необходимом для восприятия виде. Кроме этого процесс организации комплексной защиты информационных ресурсов и процесс ведения информационной войны сопровождается многочисленными неточностями и неопределённостями, что также влияет на построение и реализацию эффективной комплексной защиты. Специфика исследуемой области такова, что предлагаемый метод фактически должен быть формализован в виде комплексной системы защиты информации (КСЗИ). С целью эффективного обеспечения и управления комплексной информационной безопасностью рационально этот процесс рассматривать на этапах проектирования и эксплуатации КСЗИ. Создание комплексных систем защиты информации регламентируется известным перечнем нормативных документов, таких как: НД ТЗІ 3.7-003 – 2005 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі", НД ТЗ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на стоворення комплексної системи захисту інформації в автоматизованій системі», НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Выполнение этих нормативных документов, безусловно, гарантирует построение эффективной КСЗИ. Однако такой подход даст нам решение только 1-й задачи, т.е. защите информационных ресурсов, решение же второй задачи – защите от негативного информационно-психологического влияния – остаётся практически незатронутой. Поэтому для преодоления указанных проблем и в развитие теоретико-практических положений, изложенных в указанной научной литературе и нормативных документах, автором предлагается метод, применение которого обеспечит гарантированный уровень комплексной информационной безопасности.

Целью исследования является обеспечение гарантированного уровня комплексной информационной безопасности для объекта защиты, который функционирует в условиях информационной войны.

Задачи исследования

Для реализации поставленной цели необходимо решить следующие задачи:

1. Выполнить анализ существующих исследований в данном направлении.
2. Разработать комбинированный и гибкий метод для управления комплексной информационной безопасностью на этапах проектирования и эксплуатации КСЗИ.

Основная часть

Все попытки нарушения информационной безопасности, которые можно трактовать как возникновение конфликтной ситуации, происходят из-за желания овладеть ресурсами конкурента [3]. Конфликт предполагает противоборство, которое в современных условиях проявляется в так называемых гибридных войнах. Информационная война является одной из составляющих гибридной войны, которая может проводиться на различных уровнях, в частности, на уровне «предприятие – регион – государство». Анализируя необходимые и достаточные условия эффективного функционирования предприятия как объекта защиты, приведём такую теорему.

Теорема. Система как объект защиты обречена на уничтожение, если ресурсы этой системы не восстанавливаются и не поддерживаются на достаточном уровне на протяжении всех этапов жизнедеятельности и не являются адекватными как внутренним, так и внешним изменениям.

Доказательство. На объекте защиты для поддержания его жизнедеятельности в течение времени t расходуются и изменяются количественно и качественно различные ресурсы, такие как: информационные ресурсы, оборудование и технологии, персонал и помещения. Таким образом, можно записать, что :

$$R(t) = (I(t), O(t), P(t), PM(t)) \to 0,$$

где t – время функционирования объекта защиты, $R(t)$ - интегральные ресурсы объекта защиты, $I(t)$ – информационные ресурсы, $O(t)$ – оборудование и технологии, $P(t)$ - персонал, $PM(t)$ – помещения объекта защиты.

Под воздействием информационных атак на техническую составляющую и информационно-психологического воздействия на социальную составляющую СТС, будут нарушены как отдельные элементы объекта защиты, так и связи между этими элементами. Это приведёт к тому, что уровни защищённости соответствующих ресурсов и соответствия их количественному и качественному

уровням станут меньше допустимого и выйдут за пределы точки бифуркации.

$$(I(t), O(t), P(t), PM(t)) < R_{\partial on} \text{ или } R(t) < R(t)_{\partial on},$$

где $R_{\partial on}$, является предельно допустимым уровнем защищённости соответствующих ресурсов и соответствующим индикатором о недопустимости или невозможности для дальнейшего функционирования объекта защиты.

Приведённая теорема показывает, что для эффективного функционирования объекта защиты необходимо обеспечить достаточный уровень комплексной защищённости всех ресурсов объекта защиты. Данная теорема, а также теоремы, приведённые в [4] и полученные в них соотношения, позволяют разработать на их основе комбинированный и гибкий метод управления комплексной информационной безопасностью.

Метод управления комплексной информационной безопасностью

Комбинированный и гибкий метод, сочетающий в себе возможности обеспечения комплексной информационной безопасности на этапе проектирования и этапе эксплуатации КСЗИ, предлагается строить на базе математического аппарата теории нечётких множеств и теории статистики. Как любая система, КСЗИ имеет определённые этапы жизнедеятельности, важнейшим из которых является этап проектирования, который в большинстве случаев характеризуется разного рода неопределённостью. Отсюда вытекает обоснованная необходимость применения математического аппарата нечётких множеств, который позволит формализовать оценки возможных угроз, рангов, рисков и т.д. Решение задачи оценивания и управления комплексной информационной безопасностью предложен в работе [5]. Следует отметить, что при наличии достаточной статистики этап проектирования также может сопровождаться вероятностными моделями. На этапе эксплуатации возникает возможность, используя средства мониторинга, накапливать статистические данные и обоснованно использовать вероятностные оценки и соответствующие модели. Поэтому предлагаемый метод управления комплексной информационной безопасностью должен быть гибким и комбинированым (F[lexible]C[ombined] – метод), сочетая в себе возможность работы как с нечёткими данными, так и с вероятностными оценками. Применительно к решению задачи управления комплексной информационной безопасностью, которая, в свою очередь, обеспечивается решением задач оценивания и обеспечения гарантированного уровня комплексной информационной безопасности, последовательность действий предлагается представить в виде множества операций: ***определение проблем и целей, мониторинг, анализ, подготовка и принятие решения, внедрение и сопровождение.*** С учётом специфики этапов проектирования и эксплуатации перечисленные операции сопровождаются соответствующим математическим и нормативно-правовым обеспечением. Схематическое представление последовательности предложенных операций представлено на рис. 1.

Представленные операции предполагают выполнение таких функций:

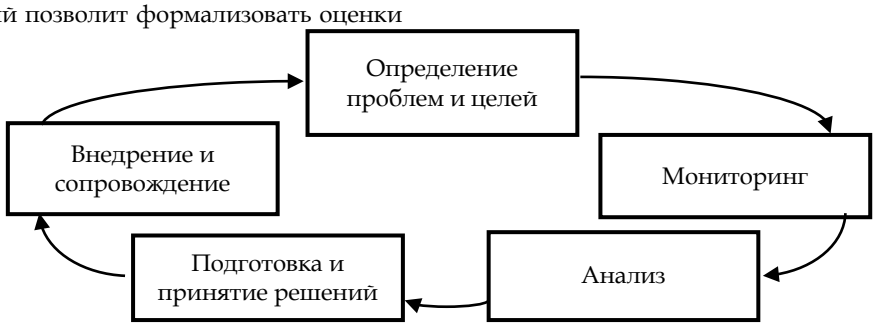

Рис. 1.Базовые операции FC- метода

Определение целей проекта на создание КСЗИ предполагает разработку ТЗ, согласование требований заказчика.

Мониторинг предполагает своевременное обнаружение угроз, уязвимостей, причин их возникновения как для собственных информационных ресурсов, так и выявление возможностей и признаков проведения информационно-психологических операций со стороны конкурентов.

Анализ предполагает выявление причинно-следственной связи возникновения и реализации угрозы через использование той или иной уязвимости и оценки вероятных рисков, связанных с данным сценарием развития событий. Представленный метод предполагает проведение анализа как на этапе проектирования КСЗИ, так и на этапе эксплуатации. Анализ угроз обязательно включает анализ угроз проведения множества $\{IP_i\}$ специальных информационно-психологических операций, где i - тип информационно-психологического воздействия.

Подготовка и принятие решений предполагает формализацию критерия принятия решения, формирования множества возможных решений и принятие окончательного решения. Принятие решения реализуется в виде синтеза оптимальной КСЗИ и разработки политики информационной безопасности (ПИБ). На этапе проектирования системы решение может формироваться на основе нечётких или качественных оценок. На этапе эксплуатации ППР может формироваться как на основе экспертных, так

и на основе вероятностных оценок. Принятое решение учитывает необходимость защиты от специальных информационно-психологических операций.

Внедрение и сопровождение характеризуются организацией контроля за выполнением ПИБ и сопровождением работы КСЗИ.

Цикл операций, показанный на рис.1., представляет систематизированную совокупность моделей, инструментов, различных средств и организационных решений, которые, собственно, и формализуют предложенный метод. Это позволяет решить следующие задачи: выявить потенциальные угрозы и уязвимости, которые могут быть использованы для реализации этих угроз; определить причинно-следственные связи триады – угроза-уязвимость-последствия; принять эффективное решение по нейтрализации угроз с последующим представлением политики информационной безопасности.

Практическая реализация операций на этапе проектирования и этапе эксплуатации КСЗИ предполагает соответствующую формализацию всех перечисленных процессов применения нормативно-правового обеспечения и соответствующего организационного сопровождения. Этап проектирования сопровождается выполнением таких операций:

Определение целей и задач на создание КСЗИ, систематизация требований заказчика, согласование всех вопросов.

Анализ и идентификация множества как внешних, так и внутренних угроз и уязвимостей, а также информационной среды на предмет возможности проведения специальных информационно-психологических операций со стороны конкурентов.

Синтез – техническая и технологическая реализация системы, которая гарантирует на этапе проектирования необходимый уровень комплексной защищённости информационных и других ресурсов объекта защиты.

Этап проектирования завершается практически созданием модели КСЗИ, которая на этапе внедрения реализуется в функционирующую систему.

Этап эксплуатации обеспечивается выполнением таких операций:

Мониторинг на этапе эксплуатации предполагает обнаружение угроз и уязвимостей в реальном времени. Выявление причин и источников их возникновения как для собственных ресурсов, так и выявление возможностей и наличия признаков проведения информационно-психологических операций со стороны конкурентов.

Анализ предполагает идентификацию множества внешних и внутренних угроз, а также информационной среды на предмет возможности проведения специальных информационно-психологических операций со стороны конкурентов.

Моделирование реальной ситуации обеспечивает получение текущих значений контролируемых параметров состояния объекта защиты с определением причин и последствий их отклонений от допустимых значений.

Операция принятия решений обеспечивает для объекта защиты необходимый или достаточный уровень защищённости.

Обратная связь обеспечивает процесс адаптации КСЗИ к изменениям как внешних, так и внутренних угроз и тем самым гарантирует необходимый уровень защищённости всех ресурсов.

На этапе эксплуатации объекта защиты, используя результаты операции мониторинга, на протяжении определённого времени накапливается достаточная статистика, на базе которой предлагается использовать подход метода «6-сигм». Этот метод, в свою очередь, опирается на 6 позиций, выполнение которых определяет эффективность производственных процессов. Систематизация последовательности действий, известная под аббревиатурой DMAIC (define, measure, analyze, improve, control), представляет собой процесс алгоритмизации оценивания текущего и обеспечения необходимого уровня тех или иных параметров процесса [6].

В данном случае случайной величиной и контролируемым параметром производственного процесса является уровень информационной защищённости объекта. Используя показатели среднего значения и стандартного отклонения можно оценить вероятностную часть отклонений показателей уровня защищённости от необходимых значений контролируемого параметра. Очевидно, что для снижения количества отклонений необходимо, используя различные инструменты, средства и мероприятия, добиться снижения значения сигма. Суть метода «6-сигм» представлена на рисунке 2.

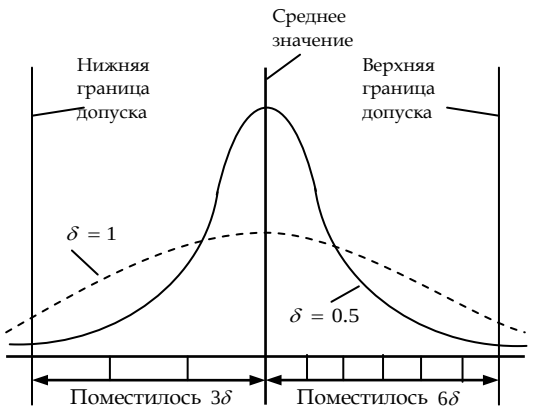

Рис 2. Графическая интерпретация метода «6-сигм»

По величине среднего значения μ и отклонения σ можно принимать решение по управлению информационной безопасностью того или иного объекта.

Выход контролируемого параметра за границы допуска говорит о недопустимых отклонениях и необходимости принятия соответствующих управленческих решений.

Обобщённая структурная модель, представляющая предложенный FC – метод, показана на рис. 3

Следует отметить, что важной задачей по организации комплексной защиты информации, согласно выше перечисленным нормативным документам, является подготовка персонала, обучение которого можно организовать с учётом накопленной статистики.

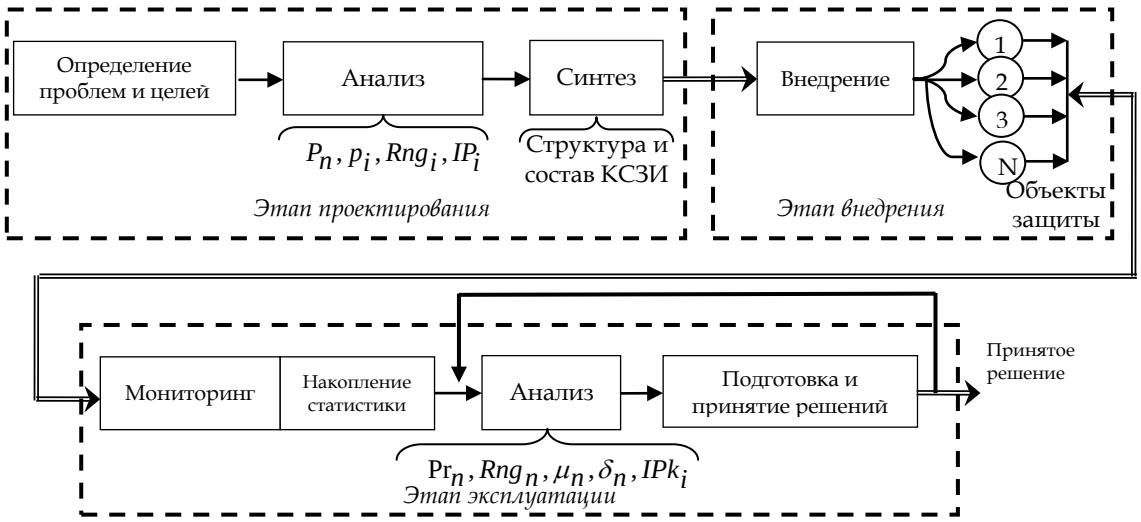

Рис.3. Структурная модель FC- метода

На рис. 3 представлено: этап проектирования, где P_n - необходимый уровень защищенности n-го объекта, p_i - вероятность возникновения i-ой угрозы, Rng_i – ранг i-ой угрозы, который определяет его значимость для общего показателя защищенности, IP_i - множество возможных информационно-психологических операций. На этапе эксплуатации, где возникает возможность управления контролируемыми параметрами по реальным их значениям на уровне «предприятие-регион-государство», Rng_n будет определять ранг n-го предприятия как объекта защиты, $\Pr_n$ – реальный уровень защищенности n-го объекта. Соответственно μ_n и δ_n определяют средние значения и отклонения параметра уровня защищенности для n-го объекта защиты, IPk_i – конкретный тип информационно-психологической атаки.

Пример.

В качестве примера применения FC – метода рассмотрим ситуацию управления комплексной информационной безопасностью региона. В структуре региона находятся N объектов защиты, для каждого из которых установлены значения уровней защищённости ресурсов: $P_1, P_2, ..., P_n$.

Пошаговое применение FC – метода для наглядности представим в таблице 1.

Таблица 1

Пример применения FC – метода

Выполняема операция	Результат выполнения операции	Обеспечение выполнения операции
Этап проектирования КСЗИ		
Определение проблем и целей	Разработка ТЗ, согласование всех вопросов между подрядчиком и заказчиком	Нормативно-правовое обеспечение, проектная документация
Анализ	Идентификация угроз, уязвимостей, рисков. Расчёт p_i, P_n, Rng_i. Учет возможности проведения множества информационно-психологических атак и их типов – IP_i.	Применение математического аппарата теории нечётких множеств. При наличии достаточной статистики применение аппарата теории вероятности. Нормативно-правовое обеспечение.
Синтез КСЗИ	Состав и структура КСЗИ. Политика информационной безопасности.	Критериальные оценки по оптимизации структуры и состава КСЗИ. Нормативно-правовое обеспечение.
Этап эксплуатации КСЗИ		
Мониторинг	Выявление в реальном времени угроз, уязвимостей, рисков. Накопление статистики, которая используется, в том числе и для обучения персонала.	Нормативно-правовое обеспечение. Применение специальных программных и технических средств. Проведение специальных организационных мероприятий.
Анализ	Идентификация угроз, уязвимостей, рисков в реальном времени. Расчёт $\Pr_n, Rng_n, \mu_n, \sigma_n$ с учётом накопленной статистики. Идентификация типа IPk_n информационно-психологической атаки. Сравнение текущих значений параметров с допустимыми значениями.	Нормативно-правовое обеспечение Возможность применения математического аппарата теории вероятности и математической статистики. Проведение специальных организационно-технических мероприятий для упреждения или минимизации последствий проведения информационно-психологических операций.

Окончание таблицы 1

Подготовка и принятие решения	Используя результаты анализа, реализуется принятое решение по управлению комплексной информационной безопасностью.	Нормативно-правовое обеспечение.

Выводы

Для того чтобы победить организованного и квалифицированного противника в лице хакера или группы хакеров, а также эффективно противостоять организованным информационно-психологическим операциям, разработанный метод должен быть интегрирован в системную организацию комплексного противодействия. Поэтому предложенный метод предлагается реализовать в структуре ситуационного центра (СЦ) на уровне управления комплексной информационной безопасностью «предприятие – регион – государство». Гибкость и комплексность предложенного FC-метода позволят эффективно решать задачи по комплексной защите информации, которые изложены в НД ТЗІ 1.4-001-2000 (Додаток, п.1.), с учётом специфики этапов проектирования и эксплуатации КСЗИ в условиях ведения информационной войны на уровне «предприятие-регион-государство».

Література

[1] Whitman M. Management of information security /M. Whitman, H. Mattord. – Gengage Learning, 2010. – 592p.

[2] Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А. Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

[3] Дружинин В.В. Введение в теорию конфликта / В.В. Дружинин, Д.С. Конторов, М.Д. Конторов – М.: Радио и Связь, 1989. – 288 с.

[4] Дудатьєв А.В. Теоретичні аспекти та технології керованого хаосу для реалізації комплексного інформаційного захисту соціотехнічних систем / А.В. Дудатьєв // Інформаційні технології та комп'ютерна інженерія. – 2014. – № 2(30). – С.28-32.

[5] Дудатьєв А.В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А.В. Дудатьєв // Вісник Черкаського технологічного університету. – 2008. – №1. – С. 3-8.

[6] Джордж М.Л. Бережливое производство шесть сигм в сфере услуг / М.: Л. Джордж. – М.: Альпина Бизнес Букс, 2005. – 402 с.

УДК 004.056 (045)

Дудатьєв А.В. Метод управління комплексною інформаційною безпекою

Анотація. *Функціонування будь-якого сучасного об'єкта, діяльність якого пов'язана з наданням послуг або виробництвом різної продукції, пов'язана з вирішенням актуального завдання - забезпеченням комплексної інформаційної безпеки. При цьому під забезпеченням комплексної інформаційної безпеки розуміємо вирішення двох завдань: забезпечення інформаційної безпеки або захист власних інформаційних ресурсів і захист від можливих інформаційно-психологічних впливів конкурентів. У запропонованій статті можливі порушення інформаційної безпеки розглянуті як потенційно можливі конфліктні ситуації, що можуть виникнути на різних рівнях управління і супроводжуватися різного роду протиборствами як елементами гібридної війни за ресурси. Наведено теорему, яка формалізує необхідні і достатні умови ефективного функціонування сучасного підприємства як об'єкта комплексного захисту. У статті вперше запропоновано поняття інформаційної обфускації як технології заплутування людини під час проведення спеціальних інформаційно-психологічних впливів і запропонований універсальний і гнучкий метод управління комплексною інформаційною безпекою, який враховує специфіку етапів життєдіяльності як об'єкта захисту, так і комплексної системи захисту інформації. Запропонований метод пропонується інтегрувати в структурах ситуаційних центрів, що дозволить забезпечити необхідний рівень захищеності даного об'єкта на рівні «підприємство-регіон-держава».*

Ключові слова: *комплексна інформаційна безпека, метод управління комплексною інформаційною безпекою, інформаційна війна, інформаційно-психологічна операція, інформаційна обфускація, комплексна система захисту інформації.*

Dudatyev A. Method for complex information security management

Abstract. *The functioning of any modern entity, which practice is related to the services provision or products manufacturing, concerns solving of the important task – complex information security providing. Wherein, complex information security providing is meant two tasks: information security providing or the protection of entity's information resources and the protection directed against possible information and psychological effects caused by competitors. At the article possible information security violations are considered as potentially possible conflicts, those might arise at different management levels and could be accompanied by various kinds of confrontations as elements of the hybrid war for resources gaining. The theorem is presented, which allows to formalize necessary and sufficient conditions for efficient performance of the modern enterprise as the complex protection object. The article contains the first presentation of the notion of the information obfuscation as the technology of person entanglement as a result of the special information and psychological impacts provision and it is proposed the versatile and flexible method of the complex information security management, which considers the vital activity stages peculiarities of both the protected entity and complex information protection system. The proposed method is considered to be integrated into the structure of the situational centers, which are to provide the required level of the entity protection at the scale «enterprise-region-state».*

Key words: *complex information security, method for complex information security management, information warfare, information and psychological operation, information obfuscation, complex information security system.*

Отримано *25 травня 2015 року*, затверджено редколегією *17 червня 2015 року*