фотоприёмника и переносимой по волокну мощности определить место расположения приёмника для регистрации оптического излучения. Из полученных результатов следует, что с увеличением показателя преломления сердцевины волокна мощность на входе приёмника резко уменьшается. Поэтому с целью защиты информации, передаваемой по оптоволокну, целесообразно диэлектрическую проницаемость сердцевины брать по возможности больше.

Список литературы:

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации.- К.:Юниор,2003.-502с.
2. Клебан В.А. Тенденции развития специальной техники разведывательного назначения //Защита информации. Сб. научн. тр.-К.:КМУГА,1998.- С.172-178.
3. Каток.В.Б., Манько А.А. Проблемы защиты информации в волоконно-оптических линиях связи //Материалы международной научно-технической конференции "Повышение эффективности систем защиты информации".- К.:КМУГА,1997.-С.135-138.
4. D. Marcuse. Theory of Dielectric Optical Waveguides. Academic Press,2005.-642p.
5. Jeff Hecht.. Understanding Fiber Optics. Prentice Hall, 2005.-800p.
6. Листвин А.В. Оптические волокна для линий связи - М.:Лесарарт,2003.-288с.
7. Гончаренко А.М., Карпенко В.А. Основы теории оптических волноводов.- М.:УРСС,2004.-204с.
8. Козловский В.В. Цепные модели планарных оптических волноводов // Зб. науч. тр.- Севастополь.- Сев. нац. ин-т яд. энерг. и пр.- 2005.- №16.- С.115-124.
9. Козловский В.В. Цепная модель несанкционированного съёма энергии с планарного оптоволокна //Захист інформації.-2005.-Спец. випуск.-С.61-66.
10. G. Miano, A. Maffucci. Transmission Lines and Lumped Circuits (Electromagnetism). Academic Press,2001.- 479 p.

УДК 681.3.06

С.М.Головань, А.М.Давиденко,
В.О.Хорошко, Л.М.Щербак

РОЗРОБКА ПЛАНУ ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УСТАНОВІ

Вступ

Технічний захист конфіденційної інформації – це діяльність спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації [1].

Методи захисту традиційних систем – журналів обліку конфіденційної інформації та картотек – створювались на протязі десятиліть (а іноді і століть) на основі практичного досвіду. Вони не досконалі, але для них відомій ризик і недоліки захисту. Поки немає подібного досвіду в області інформаційно-телекомунікаційних систем. Швидкі темпи інформатизації не дають часу на розробку і дослідження роботоздатності систем захисту інформації від несанкціонованого доступу.

Прийнято розрізняти два основних напрями технічного захисту конфіденційної інформації в інформаційній системі – захист інформаційної системи та інформації що обробляється від несанкціонованого доступу і захист інформації від витоку технічними каналами.

Під політикою безпеки конфіденційної інформації слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямований на захист конфіденційної інформації від певних загроз. Термін „політика безпеки" може бути застосовано щодо установи, інформаційної системи, послуги, що реалізується системою (набору функцій) тощо. Чим дрібніший об'єкт, відносно якого

застосовується даний термін, тим конкретнішим і формальніше стають правила. Для кожної інформаційної системи політика безпеки конфіденційної інформації може бути індивідуальною і залежить від технології обробки інформації, що реалізується, особливостей інформаційної системи, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама інформаційна система може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій системі буде складеною із її частин, що відповідають різним технологіям захисту конфіденційної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

План забезпечення технічного захисту конфіденційної інформації

Зупинимось на основному питанні даної роботи – плану забезпечення технічного захисту конфіденційної інформації котрий є документом згідно з якими здійснюється організація захисту конфіденційної інформації на всіх етапах життєвого циклу інформаційної системи.

План заходів щодо забезпечення технічного захисту конфіденційної інформації розробляється на підставі технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації. План забезпечення технічного захисту конфіденційної інформації визначає основні завдання захисту, загальні правила обробки інформації в інформаційній системі, мету побудови та функціонування комплексної системи захисту конфіденційної інформації. План має фіксувати на певний момент часу склад інформаційної системи, виконавці які не мають допуск та доступ до матеріальних носіїв конфіденційної інформації але беруть участь в обслуговуванні системи, склад необхідної технічної документації тощо.

План забезпечення технічного захисту конфіденційної інформації на всіх етапах життєвого циклу інформаційної системи повинен регулярно переглядатися та при необхідності змінюватись. Зміни та доповнення до нього затверджуються на тому ж рівні та в тому порядку, що і основний документ.

Наведемо варіант форми плану забезпечення технічного захисту конфіденційної інформації на всіх етапах життєвого циклу інформаційної системи, а саме запропонуємо електронний варіант форми плану [2].

Гриф обмеження доступу
(при необхідності)

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ**
Найменування посади керівника установи (замовника) Підпис Ініціал(и), прізвище Дата	Найменування посади керівника установи (виконавця) Підпис Ініціал(и), прізвище Дата

План
забезпечення технічного захисту конфіденційної інформації на всіх етапах життєвого циклу інформаційної системи

1. Найменування теми _____ шифр _____
Тема відноситься до _____ робіт, технічне завдання, та документація до нього має гриф обмеження доступу _____, технічні параметри _____, розробляється в підрозділі _____ установи _____.
Строк виконання технічного захисту інформації з _____ до _____.
Технічний захист інформації з обмеженим доступом виконується на підставі _____
_____

(постанови, рішення, план-графік чи інші вказівки по виконанню, номер, дата)

Примітка

Керівник теми при складанні плану заходів необхідно керуватись стандартом установи: _____

2. Установа-замовник (адреса і найменування) _____

3. Адреса і найменування співвиконавця за темою (характер виконуваної роботи, керівник роботи, найменування посади, інформованість про роботи, що виконуються за темою) _____

4. Виконавці які мають допуск та доступ до матеріальних носіїв конфіденційної інформації

Посада	Прізвище і ініціали	Місце роботи (відділ, цех тощо)	Форма допуску

5. Виконавці які не мають допуск та доступ до матеріальних носіїв конфіденційної інформації і беруть участь в технічному обслуговуванні за темою

Посада	Прізвище і ініціали	Місце роботи (відділ, цех тощо)	Примітка

6. Порядок користування матеріальними носіями конфіденційної інформації

Вказується:

– документація яка видається для роботи;

– з дозволу (керівника установи, начальника відділу тощо)

7. Порядок ознайомлення з матеріалами розробника:

– представника замовника _____

– представників сторонніх установ _____

8. Порядок листування за темою _____

9. Порядок проведення нарад (приміщення, № кімнати, об'єм інформації) _____

10.Перелік конфіденційних документів, необхідних при виконанні

Назва документу	Примітка

Примітка

Керівник теми при визначенні необхідного виду конфіденційної документації в залежності від характеру розробки необхідно керуватись стандартом установи: _____

11. Порядок опублікування та передачі документів стороннім установам _____

12. Заходи щодо технічного захисту інформації початок з _____ до _____ згідно з інструкціями щодо технічного захисту інформації інв. № _____

а) відомості, що підлягають захисту за допомогою технічних засобів _____

б) види та засоби технічного захисту інформації _____

13. ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ ПО ТЕХНІЧНОМУ ЗАХИСТУ ІНФОРМАЦІЇ

Етапи побудови системи захисту інформації з обмеженим доступом	Гриф обмеження доступу	Строк проведення робіт
Визначення та аналіз загроз		
Розроблення системи захисту інформації з		

обмеженим доступом		
Реалізація плану захисту інформації з обмеженим доступом		
Контроль функціонування та керування системою захисту інформації з обмеженим доступом		

На першому етапі необхідно здійснити аналіз об'єктів захисту, ситуаційний план, умов функціонування установи, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

На другому етапі слід розробити план технічного захисту інформації, що містить організаційні, первинні технічні та основні технічні заходи захисту конфіденційної інформації, визначити зони безпеки інформації.

На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту конфіденційної інформації, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

На четвертому етапі слід провести аналіз функціонування системи захисту інформації, перевірку виконання заходів технічного захисту інформації, контроль ефективності захисту, підготувати та видати засадчі дані для керування системою захисту конфіденційною інформацією.

14. ПОЕТАПНО НА ВЕСЬ ПЕРІОД РОБОТИ

Відділ, цех, номери кімнат, в яких проводиться розробка, складання, монтаж, випробування	Виконавці (прізвище, ініціали, підрозділ)	Забезпечення заходів режиму на період робіт (при наявності охоронної сигналізації, шифр-замка, списку осіб які мають доступ до приміщення тощо)	Примітка

15. Коли закінчена робота за темою. Які підсумкові документи видані, їх облікові номери. Список осіб, яким дозволено користуватися матеріалами роботи _____ .

Від замовника

Керівник роботи
Підпис Ініціал(и), прізвище

Начальник підрозділу
Підпис Ініціал(и), прізвище

Від виконавця

Керівник роботи
Підпис Ініціал(и), прізвище

Начальник підрозділу
Підпис Ініціал(и), прізвище

При виконанні робіт забороняється:

– ознайомлення із конфіденційними матеріалами представників інших установ і співробітників не працюючих за цією темою;

– залучати інші установи для виконання робіт;

– використовувати матеріали, отримані при виконанні робіт в статтях, дисертаціях, виступах на симпозіумах, конференціях тощо.

Для технічного захисту конфіденційної інформації слід застосовувати заходи приховування або заходи технічної дезінформації.

Заходи захисту інформації з обмеженим доступом повинні:

– бути відповідними загрозам;

– бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів і обмежень, що вносяться ними;

– забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здіснення загроз.

Рівень захисту конфіденційної інформації визначується системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог технічного захисту конфіденційної інформації.

Мінімально необхідний рівень захисту конфіденційної інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту конфіденційної інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

Порядок розрахунку та інструментального визначення зон безпеки конфіденційної інформації, реалізація заходів технічного захисту конфіденційної інформації, розрахунку ефективності захисту та порядку атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з технічного захисту конфіденційної інформації.

Технічне завдання на створення комплексної системи захисту інформації в інформаційній системі є засадчим організаційно-технічним документом для виконання робіт щодо забезпечення захисту конфіденційної інформації в системі.

Технічне завдання на комплексну систему захисту конфіденційної інформації розробляється у разі необхідності розробки або модернізації комплексної системи захисту конфіденційної інформації існуючої (що функціонує) інформаційною системою. В разі розробки комплексної системи захисту конфіденційної інформації в процесі проектування інформаційної системи допускається оформлення вимог захисту конфіденційної інформації в інформаційній системі у вигляді окремого (часткового) технічного завдання, доповнення до загального технічного завдання на інформаційну систему або розділу загального технічного завдання на інформаційну систему.

Технічне завдання на комплексну систему захисту конфіденційної інформації повинно розроблятись з урахуванням комплексного підходу до побудови комплексної системи захисту конфіденційної інформації, який передбачає об'єднання в єдину систему усіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу інформаційної системи.

В технічному завдання на комплексну систему захисту інформації викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в інформаційній системі. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза інформаційною системою у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в технічне завдання на комплексну систему захисту інформації, може бути для кожної конкретної інформаційної системи як розширений, так і скорочений.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Висновки

Викладені загальні підходи до побудови плану забезпечення технічного захисту конфіденційної інформації на всіх етапах життєвого циклу інформаційної системи та запропонуємо комп'ютерний варіант форми плану.

Список літератури:

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99, ДСТЗІ СБ України, Київ, 1999.
2. Закон україни "Про електронні документи та електронний документообіг": Закон України від 22.05.2003 № 851-IV // Відомості Верховної Ради України. – 2003. – № 35. – Ст. 275.

УДК 338.47:37.014

Н.Ю.Кривицкая,
А.В.Титов, В.А.Хорошко

ПРИНЯТИЕ РЕШЕНИЙ ПО ОЦЕНКЕ ИНВЕСТИЦИЙ ПРИ НАЛИЧИИ УГРОЗ И РИСКОВ

Коммерческая целевая программа (КЦП) инвестиционных процессов представляет собой совокупность мероприятий, называем «проектами», объединенных единством глобальной цели и общими ресурсами [1,2]. Основные задачи разработки сложных КЦП - отбор проектов, включаемых в программу и распределение между ресурсов. При этом КЦП, как правило, планируется на достаточно большие промежутки времени, поэтому необходимо оценивать эффективность проектов на заданном интервале времени.

При разработке КЦП следует учитывать, возможность возникновения угроз и рисков, анализировать их влияние и на этой основе предусматривать меры по их парированию.

При формировании КЦП с учетом угроз и рисков возникают следующие задачи:

- определение количественных характеристик влияния угроз и рисков на эффективность КЦП;
- определение количественных показателей относительной эффективности проектов при наличии угроз и рисков;
- распределение ресурсов между средствами парирования угроз и рисков и проектами, имеющих «созидательную» направленность.

Известные методы решения первой задачи предусматривают идентификацию рисков (качественный анализ), а также оценивание вероятностей и размеров возможного ущерба (количественный анализ) [3,4]. Однако при этом задача оценки эффективности проектов с учетом рисков не решается и остается уделом эксперта, принимающего решение ***(ЭПР)***. Более того, определение ущерба в абсолютном измерении (например, денежном) часто затруднено для сложных КЦП гуманитарной и социальной направленности.

Метод решения задачи оценки относительной эффективности проектов при наличии угроз и рисков естественно разрабатывается на основе методов решения данной задачи без учета этих факторов. Наибольшее распространение в настоящее время получены мультикритериальные методы оценки проектов [5-9]. Область их применения ограничивается двумя необходимыми условиями, которым должна удовлетворять конкретная задача.

Первое условие – наличие множества критериев, по каждому из которых можно оценить каждую альтернативу. Второе – способность ***ЭПР*** оценить тем или иным образом каждую альтернативу по каждому критерию, т.е. полностью «владеет проблемой».

Первое условие в большинстве случаев формирования сложных ***КЦП*** не выполняется из-за существенного различия природы проектов, входящих в них. Выполнение второго условия проблематично, когда выбор наилучшей альтернативы из нескольких сотен или ранжирование такого количества альтернатив требует учета их оценок по нескольким десяткам взаимосвязанных критериев. Такая ситуация имеет место при принятии решений по формированию сложных комплексных целевых программ государственного масштаба, программ развития образования.

Поэтому методы поддержки принятия решений при формировании КЦП в условиях угроз и рисков будем разрабатывать путем модификации методов нецелевого оценивания альтернатив [1,2,10]. При поддержке решений по разработке КЦП относительная эффективность проектов должна оцениваться как функция времени, заданная на интервале планирования [10]. Поэтому возможность учета фактора времени при оценке проектов КЦП