УДК 621.391.3

В.Я. Воропаєва (канд. техн. наук, доц.), І.Л. Щербов, Е.Д. Хаустова
ДВНЗ «Донецький національний технічний університет», м. Донецьк
кафедра автоматики і телекомунікацій, кафедра радіотехніки та захисту інформації
e-mail: voropayeva@donntu.edu.ua, schil@rtf.donntu.edu.ua, elvira123321@mail.ru

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ МОДЕЛІ «PLAN-DO-CHECK-ACT»

Проведено аналіз порядку прийняття рішення щодо управління інформаційною безпекою ІТС на основі моделі «Plan-Do-Check-Act». Розглянуті загрози для інформаційної безпеки ІТС, що можуть бути реалізовані з використанням протоколів міжмережевої взаємодії, їх вплив на властивості інформації. Запропоновано порядок вибору засобу захисту з урахуванням визначених критеріїв та обмежень.

Ключові слова: *інформаційно-телекомунікаційна система, протокол міжмережевої взаємодії, управління інформаційною безпекою ІТС, модель «Plan-Do-Check-Act»..*

Загальна постановка проблеми

Використання інформаційних технологій в процесах державного управління, керування бізнесом, виробничими процесами, задоволення потреб громадян мати вільний доступ до інформації сприяє розвитку інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (ІТС). Поширення інфраструктури ІТС дозволяє скоротити відстані між взаємодіючими суб'єктами, зменшити час на обмін інформацією і, як наслідок, дає змогу прискорити процес прийняття управлінських рішень в органах державного управління, місцевого самоврядування та бізнесі. При цьому гостро постають проблеми забезпечення інформаційної безпеки як в мережах загального користування [1] так і в корпоративних або мережах спеціального призначення [2].

Прикладом вирішення питання державного управління з використанням ІТС та забезпеченням гарантованого рівня інформаційної безпеки є створення на підставі Постанови Кабінету Міністрів від 13.07.2011 р. № 752 в Міністерстві освіти і науки України Єдиної державної електронної бази з питань освіти (ЄДЕБО), яка є автоматизованою системою збирання, верифікації, оброблення, зберігання та захисту даних [3].

Розподілене розташування суб'єктів відносин, пов'язаних поставленою метою забезпечення потреби фізичних та юридичних осіб щодо надання та отримання освітніх послуг, вимагає оптимального проектування та ефективного управління інформаційною безпекою в ІТС, що задіяна для функціонування даної електронної бази.

Постановка завдань дослідження

Для вирішення сформульованого завдання управління інформаційною безпекою ІТС її слід розглядати як складну систему, що включає значну кількість взаємопов'язаних інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. При вирішенні даного завдання виникає ряд проблем, найбільш складні з яких є:

- координація дій між окремими складовими, які належать різним власникам;

- вплив зовнішніх та внутрішніх деструктивних факторів;
- обмежені фінансові можливості.

Аналізуючи фактори, що впливають на процес вибору рішення щодо управління інформаційною безпекою ІТС, можна зробити висновок, що окрема взята організація, задіяна у процесі експлуатації ІТС, не в змозі вирішити дану проблему самостійно. Проте вибрати оптимальне управлінське рішення на окремих ділянках ІТС – це завдання, що може і має бути виконано. Такими ділянками можуть бути інформаційні системи (ІС) вищих навчальних закладів, Українська науково-освітня телекомунікаційна мережа УРАН та інші освітні установи, що мають доступ до ЄДЕБО. Для вирішення завдання управління інформаційною безпекою ІТС слід визначити єдині правила, якими б керувалися усі користувачі ЄДЕБО.

Безумовно, при виборі таких правил необхідно враховувати нормативно-правові документи законодавства України, рекомендації Міжнародного союзу електрозв'язку серії X «Мережі передачі даних і взаємозв'язок відкритих мереж», ISO/IEC 27001 «Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації» та інші нормативно-правові документи і рекомендації.

Однак існуючі законодавчі акти, стандарти і рекомендації не дають готової відповіді, як керувати інформаційною безпекою конкретної ІТС під час її створення та експлуатації, тому, що кожна ІТС унікальна і має свої особливості.

Тому стає актуальним питання вдосконалення методів управління інформаційною безпекою ІТС для окремо взятих установ та організацій.

Вирішення завдань і результати дослідження

Управління інформаційною безпекою ІТС – це динамічний, циклічний процес, який повинен враховувати завдання, що виникають відповідно до етапів життєвого циклу ІТС (створення та введення в експлуатацію, експлуатація, виведення із експлуатації). Відповідно, на кожному етапі життєвого циклу ІТС, необхідно приймати управлінські рішення вимоги до яких можна сформулювати наступним чином.

1. Рішення має бути прийнято на базі принципово об'єктивного проектування незалежно від вподобань і кваліфікаційних властивостей особи, яка приймає рішення (ОПР).

2. Рішення повинно прийматися з врахуванням можливих змін методів та засобів захисту або умов життєдіяльності системи [4].

3. Рішення заслуговує затвердження, якщо у визначений термін часу повторний незалежний аналіз умов, що вплинули на його прийняття, дає однаковий результат [5].

Останнім часом все частіше у процесі управління інформаційною безпекою ІТС застосовується стандарт ISO/IEC 27001 «Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації». Рекомендації даного стандарту базуються на використанні моделі «Plan-Do-Check-Act» (PDCA) (див. рис.1) [6].

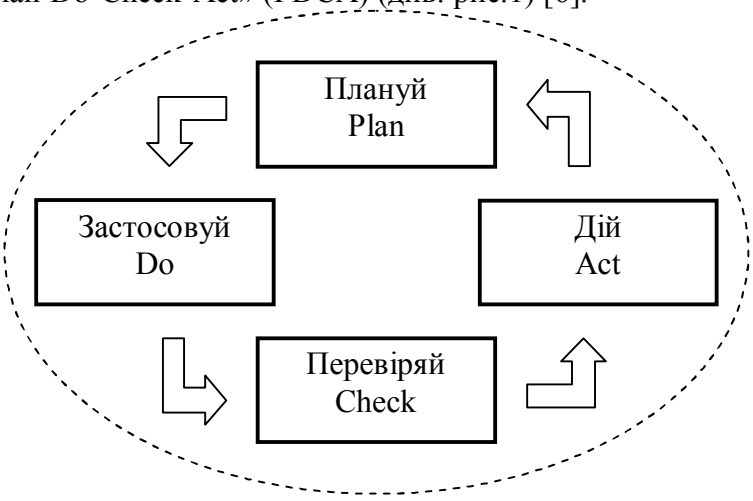

Рисунок 1 — Модель «Plan-Do-Check-Act»

Використовуючи дану модель для етапу створення та введення в експлуатацію ІТС необхідно вирішити наступні задачі управління інформаційною безпекою ІТС:

- на етапі планування (Plan) здійснюється розробка політики безпеки, оцінка ризиків, визначення цілій, процесів та процедур щодо управління інформаційною безпекою;
- на етапі застосування (Do) виконуються заходи щодо реалізації поставлених цілій, процесів та процедур щодо управління інформаційною безпекою;
- на етапі перевірки (Check) визначається відповідність реалізованих заходів, процесів та процедур цілям визначеним у політиці безпеки;
- на етапі дій (Act) здійснюється коректування запланованих і реалізованих рішень з метою вдосконалення системи управління інформаційної безпеки ІТС.

При управлінні інформаційною безпекою ІТС розглядається як складна за архітектурою, з великою кількістю компонентів система. І для кожної окремої складової даної системи визначаються правила, процеси та процедури по її управлінню, що дозволяє в свою чергу прийняти управлінське рішення, вимоги до якого було сформульовано раніше.

Розглянемо управління інформаційною безпекою ІТС при реалізації першого етапу моделі PDCA, а саме на етапі планування (Plan), на прикладі прийняття рішення щодо вибору програмних та програмно-апаратних засобів захисту ІТС від загроз, що можуть бути реалізовані з використанням протоколів міжмережевої взаємодії.

Для початку приймаємо рішення щодо варіанту захисту ІТС. Відповідно до п. 3.2 ДСТУ 3396.1 для захисту інформації може бути вибрано один із варіантів [7]:

- досягнення необхідного рівня захисту інформації з обмеженим доступом (ІзОД) за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності (ІД);
- досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;
- досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Умови рівня захисту персональних даних затверджені наказом Міністерства юстиції України від 30.12.2011 № 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних». Загальні вимоги щодо захисту персональних даних визначені в Законі України "Про захист інформації в інформаційно-телекомунікаційних системах" та в Правилах забезпечення захисту інформації в інформаційно-телекомунікаційних системах, що затверджені постановою Кабінету міністрів України від 29.03.2006 № 373. Враховуючи вимоги зазначених документів, а також факт наявності в розглянутій ІТС інформації, що містить персональні дані фізичної особи, слід зупинити вибір на третьому варіанті захисту інформації.

Визначившись з варіантом захисту, переходимо до аналізу загроз інформації в ІТС. Аналіз загроз починається з обстеження ІТС. Типову структуру ІТС вищого навчального закладу представлено на рисунку 2.

Досить часто окремі корпуси та структурні підрозділи університетів розташовані на значній відстані один від одного, що призводить до використання в корпоративній телекомунікаційній мережі ділянок публічних мереж, зокрема Інтернет. Розподіл окремих складових елементів ІТС (серверів, автоматизованих робочих місць АРМ) за місцем розташування призводить до того, що обмін даними необхідно проводити по телекомунікаційних каналах, які знаходяться за межами контрольованої території. А це означає, що місць, де необхідно проводити заходи для забезпечення інформаційної безпеки ІТС, може бути значна кількість.

При цьому слід враховувати, що інформація, яка зберігається на різних серверах (в окремих випадках на АРМ), може носити різний рівень обмеження доступу; відрізнятися за об'ємом даних, що зберігаються; мати різні вимоги щодо терміну представлення користувачу та інше. Тому виходячи із правила – вартість захисту інформації не повинна

перевищувати вартість самої інформації – необхідно в кожному окремому випадку приймати обґрунтоване рішення щодо вибору засобу захисту, відповідно до критичності інформації та можливих загроз.

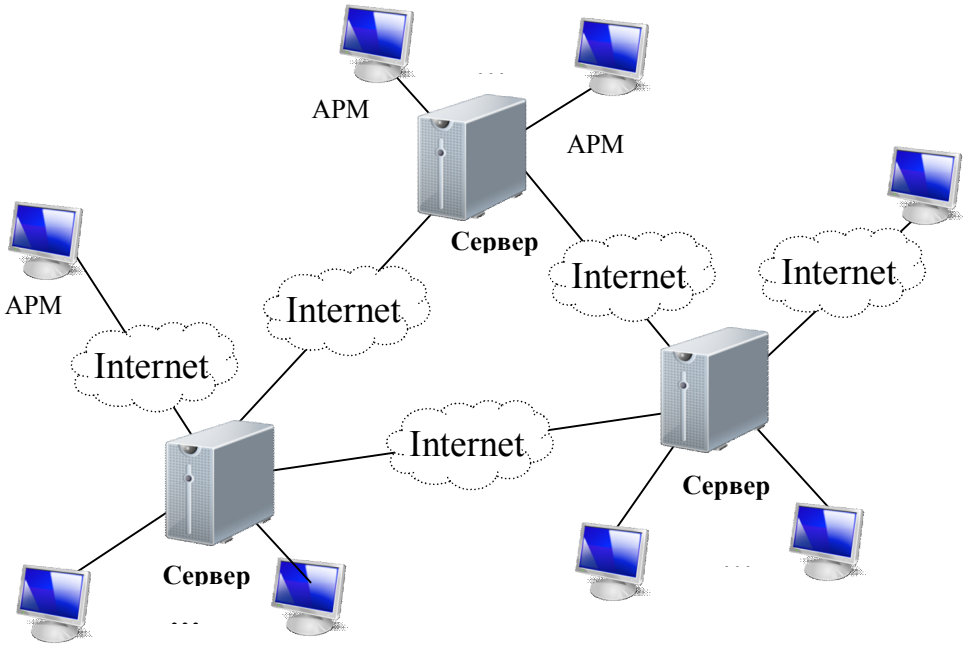

Рисунок 2 — Типова структура ІТС

Найбільш поширені загрози для інформаційної безпеки ІТС, що можуть бути реалізовані з використанням протоколів міжмережевої взаємодії [6], та узагальнена оцінка їхнього впливу на основні властивості інформації (конфіденційність, цілісність, доступність або спостереженість) представлено в таблиці 1. Слід розуміти, що не всі загрози ІТС можуть бути реалізовані в повній мірі; один і той же тип реалізованої загрози може нанести значний або незначний за своїми наслідками збиток; реалізація окремих загроз може зовсім не нанести шкоду ІТС. Тому, для прийняття рішення щодо управління інформаційною безпекою при виборі захисних мір, слід визначитися з тою долею ризику, що несе в собі загроза для інформації в разі її реалізації.

Таблиця 1

Загрози для інформаційної безпеки ІТС

№ k	Загрози (threat)	Конфіденційність (confidentiality)	Цілісність (integrity)	Доступність (availability)	Спостереженість (accountability)	Ваговий коефіцієнт
1	Аналіз протоколів	c_1	i_1	a_1	s_1	p_1
2	Сканування мереж	c_2	i_2	a_2	s_2	p_2
3	Автоматичний підбір паролів	c_3	i_3	a_3	s_3	p_3
4	Spoofing	c_4	i_4	a_4	s_4	p_4
5	Захоплення мережевих підключень	c_5	i_5	a_5	s_5	p_5
6	Підміна мережевих об'єктів	c_6	i_6	a_6	s_6	p_6
7	Розподілена відмова в обслуговуванні	c_7	i_7	a_7	s_7	p_7
8	Віддалене проникнення	c_8	i_8	a_8	s_8	p_8

В таблиці позначено c_k – оцінка впливу *k-ї* загрози на конфіденційність інформації, чисельно визначається за запропонованою нижче п'яти бальною шкалою; i_k, a_k та s_k – оцінки впливу *k-ї* загрози на цілісність, доступність та спостереженість інформації відповідно, чисельно визначаються аналогічно; ваговий коефіцієнт p_k визначає частку появи даної загрози відносно усієї сукупності загроз та може обчислюватися на основі аналізу статистики функціонування ІТС або з використанням відомих методик прогнозування. Для вагового коефіцієнту виконуються наступні умови:

$$\sum_{k=1}^{n} p_k = 1, \qquad 0 \le p_k \le 1 \qquad (1)$$

Визначення рівня небезпеки загрози необхідно проводити експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом залучення спеціалістів структурних підрозділів, в інтересах яких буде експлуатуватися ІТС. Оцінка повинна складатись з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості ІТС внаслідок реалізації загрози [7, 8]. Для оцінки загрози рекомендується вводити декілька дискретних ступенів (градацій).

Визначення рівня небезпеки загрози для властивостей інформації будемо проводити за п'яти бальною шкалою:

0 – реалізована загроза не несе збитків для ІТС;

0,25 – реалізована загроза несе не значні збитки;

0,5 – реалізована загроза несе середні збитки;

0,75 – реалізована загроза несе значні збитки;

1,0 – реалізована загроза несе значні збитки, які суттєво загрожують ІТС.

Тоді визначення рівня небезпеки (threat) T_k *k-ї* загрози для властивостей інформації, що циркулює в ІТС, здійснюємо за формулою:

$$T_k = \frac{\{c_k + i_k + a_k + s_k\}}{4} \cdot p_k . \qquad (2)$$

Формули (1) і (2) дозволяють виділити найбільш вагомі загрози з урахуванням як рівня небезпеки за рахунок впливу загроз на певні властивості інформації, так і відносної частоти появи тієї чи іншої загрози. Тепер визначившись з рівнем небезпеки різних видів загроз, можна приступити до вибору програмних та програмно-апаратних засобів захисту.

Останні розрізняються за своїм призначенням та місцем встановлення, а також, рівнем обмежень видів інформаційної діяльності, що обумовлені принципами захисту, які в них реалізовані [9]. Зробимо короткий огляд деяких з них.

Мережевий екран (Firewall) – комплекс програмних або програмно-апаратних засобів, призначений для контролю та фільтрації у відповідності з певними правилами трафіку, що проходить через нього. Як правило, встановлюється з метою захисту ІТС від несанкціонованого доступу. Забезпечує також реєстрацію спроб зондування або атак на вузли захищеної мережі. Але не захищає від внутрішніх загроз (зокрема, витоку даних) та вірусів.

VPN (Virtual Private Network) – віртуальні приватні мережі, організовані у вигляді зашифрованого тунелю, що йде над публічними мережами, зокрема Інтернет. Завдяки використанню розвинутих засобів криптографії (шифрування, ідентифікації, аутентифікації, системи відкритих ключів) VPN дає більш захищену логічну мережу, порівняно з базовою мережею, канали якої використовуються для створення VPN з'єднань.

Intrusion Detection System (IDS) або система виявлення вторгнень (СВВ) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через

Інтернет. Системи виявлення вторгнень забезпечують додатковий рівень захисту ІТС за рахунок виявлення атак та різних способів реагування на них – від найпростіших звітів до активного втручання при визначенні вторгнення.

Антивірусна програма (антивірус) – будь-яка програма для виявлення комп'ютерних вірусів, а також небажаних (шкідливих) програм взагалі і відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараження (модифікації) файлів або операційної системи шкідливим кодом.

Виходячи із функцій, які виконують програмні та програмно-апаратні засоби захисту, а також із рівня небезпеки загрози для властивостей інформації, що обробляється на окремому сервері (АРМ), ми можемо визначити очікувану захищеність ІТС Q від сукупності ймовірних загроз певним засобом захисту:

$$Q = \sum \frac{\{c_k + i_k + a_k + s_k\}}{4} \cdot p_k \cdot z_k \qquad (3)$$

де z_k – ймовірність подолання *k-ї* загрози певним засобом захисту.

Таким чином, формула (3) дозволяє зробити підрахунок очікуваної захищеності ІТС від сукупності ймовірних загроз певним засобом захисту для кожної частини ІТС, де необхідно визначитися зі способом забезпечення інформаційної безпеки. Як було зазначено, для розглянутої ІТС слід вибирати варіант максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД. Тому із розглянутих програмних та програмно-апаратних засобів захисту слід вибрати той, що в конкретному випадку дає максимальне значення захищеності Q.

Висновки

1. Рекомендовано порядок прийняття рішення щодо управління інформаційною безпекою ІТС на основі моделі PDCA.
2. Розроблено методику аналізу загроз з урахуванням рівня небезпеки загрози і відносної частоти її появи.
3. Запропоновано порядок вибору засобів захисту ІТС від загроз інформаційній безпеці, що реалізовані з використанням протоколів міжмережевої взаємодії, з урахуванням визначених критеріїв та обмежень.

Список використаної літератури

1. Воропаева В.Я. Вопросы обеспечения информационной безопасности в сетях общего пользования / В.Я. Воропаева, В.А. Попов, И.В. Стародубов // Наукові праці ДонНТУ. Серія: Обчислювальна техніка та автоматизація. – Донецьк,2000. – Вип. 20. – .. 159-165
2. Бурячок В.Л.. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В.Л. Бурячок // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С.104–114.
3. Україна. Постанови Кабінету Міністрів України. Про створення Єдиної державної електронної бази з питань освіти. [Текст]: [затверджено Кабінетом Міністрів України 13.07.2011 р]. –К.: Офіційний вісник України офіційне видання від 29.07.2011 р., № 55, стор. 37, стаття 2191, код акту 57644/2011.
4. Воропаєва В. Я. Адаптування інформаційно-телекомунікаційних систем до зовнішніх впливів / В.Я. Воропаєва, І.Л. Щербов // Наукові праці ДонНТУ. Серія: Обчислювальна техніка та автоматизація. – Донецьк: ДонНТУ, 2012. – Випуск 23 (201) – С. 83-88.
5. Луценко В. М. Система інтелектуальної підтримки прийняття рішень при проектуванні комплексних систем захисту інформації / В.М. Луценко // Наукові вісті НТУУ «КПІ». – 2010. – № 5.– С. 68–74.

6. ISO/IEC 27001 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации». ISO/IEC 27001:2005(E).
7. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. — Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=38883&cat_id=38836 .
8. Базовая модель угроз безопасности персональных даннях при их обработке в информационных системах персональных данных (выписка) [Електронний ресурс]. — Режим доступу : http://fstec.ru/component/attachments/download/289.
9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]. — Режим доступу : http://dstszi.kmu.gov.ua/ .

Надійшла до редакції:
27.04.2013р.

Рецензент:
д-р пед. наук, проф. Стефаненко П.В.

В.Я. Воропаева, И.Л. Щербов, Е.Д. Хаустова
ГВУЗ «Донецкий национальный технический университет»

Управление информационной безопасностью информационно-телекоммуникационных систем на базе модели «Plan-Do-Check-Act» *Проведен анализ порядка принятия решения по управлению информационной безопасностью информационно-телекоммуникационных систем (ИТС) на базе модели «Plan-Do-Check-Act». Рассмотрены угрозы для информационной безопасности ИТС, которые могут быть реализованы с использованием протоколов межсетевого взаимодействия, их влияние на свойства информации. Предложен порядок выбора средства защиты с учетом определенных критериев и ограничений.*

Ключевые слова: *информационно-телекоммуникационная система, протокол межсетевого взаимодействия, управление информационной безопасностью ИТС, модель «Plan-Do-Check-Act».*

V.Y. Voropayeva, I.L. Shcherbov, Ye.D. Khaustova
Donetsk National Technical University

Information and Telecommunication Systems Security Management on the Basis of "Plan-Do-Check-Act" Model. *We analyzed the sequence of decision-making in information security management of the information and telecommunications system (ITS) on the basis of PDCA model. Selection criteria and constraints that influence decision making were chosen according to ISO/IEC 27001 "Information technology. Security Techniques. Information Security. Management System", recommendations and requirements of current legislation of Ukraine. The procedure of analyzing the impact of threats on information properties and manageability of ITS system protection was proposed. The procedure is based on the analysis of vulnerability of interworking protocols, used in information and telecommunications systems, due to different types of attacks effects.*

The paper provides the procedure of discrete risk assessment for information and telecommunication systems on the basis of expert estimates of expected damage in case of threats realization. Proceeding from the principle - the cost of protection should not exceed the value of the information being protected – we suggest a technique of making control decisions on the choice of means of protection, allowing choosing software and (or) hardware protection (for each particular point of contact of local information network with the external telecommunications system) with security features implemented, which are adequate to the threats.

Keywords*: information-telecommunication system, interworking protocol, information security management system,* ***"****Plan-Do-Check-Act****"****model.***