УДК 004.056.57

Чередниченко О.Ю. (ВІТІ)
Процюк Ю.О. (ВІТІ)
Шемендюк О.В. (ВІТІ)
Мальцева І.Р. (ВІТІ)

СПОСОБИ ВДОСКОНАЛЕННЯ СХЕМ ЗАХИСТУ ВІД КІБЕРНЕТИЧНИХ АТАК В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті проаналізовано основні методи виявлення кібернетичних атак, а саме сигнатурний аналіз (метод виявлення зловживань) та метод виявлення аномалій. На основі аналізу розглянутих методів зроблено висновок, що для підвищення рівня захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах доцільно застосовувати методи на основі виявлення аномалій, оскільки саме їм притаманно виявляти кібератаки 0-day. В роботі проводиться огляд основних засобів виявлення (протидії) кібернетичних атак серед яких технології Intrusion Detection System/Intrusion Prevention System, Firewall, антивірусні програми та технології Security information and event management. На основі розглянутих засобів була представлена та проаналізована типова схема застосування засобів захисту від кібернетичних атак.

З метою покращення ефективності схеми захисту від кібернетичних атак та підвищення рівня захисту в інформаційно-телекомунікаційних системах запропоновано до розглянутої схеми додати координатор, основною метою якого буде координація дій всіх засобів з вузьким спектром всіх функцій. Крім цього пропонується до координатора подати модель вибору раціонального варіанта реагування на події порушення безпеки та представлений орієнтовний граф. Застосування такого підходу дозволить не тільки підвищити рівень кібернетичної захищеності в інформаційно-телекомунікаційних системах, а й може бути платформою для автоматичного створення експлойтів та сигнатур кібератак на основі наявних аномалій.

Ключові слова: *кібернетичні атаки, кібератака, Firewall, IPS/IDS, Антивірусний захист, SIEM, кібербезпека, кібероборона.*

Чередниченко А.Ю., Процюк Ю.А., Шемендюк А.В., Мальцева И.Р. Способы совершенствования схемы защиты от кибернетических атак в информационно-телекоммуникационных системах. *В статье проанализированы основные методы выявления кибернетических атак, а именно сигнатурный анализ (метод выявления злоупотреблений) и метод выявления аномалий. На основе анализа рассмотренных методов сделан вывод, что для повышения уровня защищенности информационных ресурсов в информационно-телекоммуникационных системах целесообразно применять методы на основе выявления аномалий, поскольку именно им свойственно проявлять кибератаки 0-day. В работе проводится обзор основных средств обнаружения (противодействия) кибернетических атак среди которых технологии Intrusion Detection System/Intrusion Prevention System, Firewall, антивирусные программы и технологии Security information and event management. На основе рассмотренных средств была представлена и проанализирована типичная схема применения средств защиты от кибернетических атак.*

С целью повышения эффективности схемы защиты от кибернетических атак и повышение уровня защиты в информационно-телекоммуникационных системах предложено к рассматриваемой схемы добавить координатор, основной целью которого будет координация действий всех средств с узким спектром всех функций. Кроме этого предлагается к координатору подать модель выбора рационального варианта реагирования на события нарушения безопасности и представлен ориентированный граф. Применение такого подхода позволит не только повысить уровень кибернетической защищенности в информационно-телекоммуникационных системах, но и может быть платформой для автоматического создания эксплоитов и сигнатур кибератак на основе имеющихся аномалий.

Ключевые слова: *кибернетические атаки, кибератака, Firewall, IPS / IDS, антивирусных защиту, SIEM, кибербезопасность, кибероборона.*

O. Cherednychenko, Y. Protsiuk, O. Shemendiuk, I. Maltseva. Ways to improve the protection against cyber-attacks in information and telecommunication systems. *The main methods of cyber-attack detection are analyzed in the article, namely signature analysis (abuse detection method) and anomaly detection method. Based on the analysis of the considered methods, it is concluded that in order to increase the level of security of information resources in information and telecommunication systems, it is advisable to apply methods based on the detection of anomalies, since it is inherent to them to detect 0-day cyber-attacks. This paper reviews the main means of detecting (counteracting) cyber attacks, including the technologies Intrusion Detection System/Intrusion Prevention System, Firewall, anti-virus programs and technologies Security information and event management. On the basis of the considered means, a typical scheme of application of the means of protection against cyber attacks was presented and analyzed.*

In order to improve the effectiveness of the scheme of protection against cyber-attacks and to increase the level of protection in the information and telecommunication systems, it is proposed to add to the scheme under consideration a coordinator, the main purpose of which will be coordination of actions of all means with a narrow spectrum of all functions. In addition, it is suggested that the coordinator submit a model for choosing a rational

response to a security breach event and provide an indicative graph. Applying this approach will not only increase the level of cyber security in information and telecommunication systems, but can also be a platform for automatically creating exploits and signatures of cyber attacks based on existing anomalies.

Key words: *cyber attacks, cyber attacks, Firewall, IPS / IDS, antivirus protection, SIEM, cybersecurity, cyber defense.*

Постановка завдання. Згідно закону України "Про основні засади забезпечення кібербезпеки України" кібератака (КА) – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

За останні 5 років Україна зазнала декількох масштабних КА різного рівня складності, які були поширені в об'єктах енергетичної інфраструктури, Міністерстві фінансів, Держказначейства, Пенсійного фонду. Було порушено роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ [1, 2]. Більша їх частина була пов'язана із війною на сході України, яка розпочалась у 2014 р. Це обумовлює необхідність вирішення задачі підвищення ефективності кібербезпеки.

Аналіз сучасних кібератак в період з 2014 по 2018 роки показав слабкий рівень кібербезпеки в країні. Серед основних атак, які були здійснені на об'єкти критичної інфраструктури, можна виділити наступні: отруєння кешу DNS та розподілена атака на відмову в обслуговуванні (DDoS-атака), ефективної протидії яким на сьогоднішній день не створено.

Аналіз останніх досліджень і публікацій [2 – 8] показав, що існує велика кількість методів та засобів захисту від атак на відмову в обслуговуванні. До основних методів виявлення (протидії) КА належать: сигнатурний аналіз (метод виявлення зловживань) та метод виявлення аномалій. До основних засобів виявлення (протидії) КА належать технології IDS/IPS (англ. Intrusion Detection System/Intrusion Prevention System, укр. Система виявлення атак (СВА)/Система запобігання атак (СЗА), антивірусні програми, мережеві екрани (Firewall). Оскільки природа кібернетичних атак є різноманітною, тому не існує єдиного підходу до захисту від всіх кібератак одночасно. У зв'язку з цим, виникає завдання пошуку ефективного рішення виявлення (протидії) КА в інформаційно-телекомунікаційних системах (ІТС).

Метою статті є вибір ефективної схеми захисту від КА та підвищення рівня захисту в ІТС.

Виклад основного матеріалу дослідження

Методи захисту від КА [2 – 5]**.** Існує дві основні групи методів аналізу подій в ІТС для виявлення атак:

виявлення зловживань (*misuse detection*);

виявлення аномалій (*anomaly detection*).

Виявлення зловживань (*сигнатурний метод*). Детектори зловживань контролюють діяльність системи, аналізуючи подію або множину подій на відповідність заздалегідь визначеному зразку (сигнатурі), що описує відому атаку. Найбільш типова форма визначення зловживань, що здебільшого використовується у комерційних продуктах, визначає кожний зразок події, що відповідає атаці, як окрему сигнатуру. Проте існують складніші підходи для виявлення зловживань, що отримали назву технологій аналізу на основі стану (state-based), які можуть використовувати єдину сигнатуру для визначення групи атак.

Переваги сигнатурного методу:

детектори зловживань є дуже ефективними для визначення атак;

детектори зловживань не створюють величезного числа помилкових повідомлень;

детектори зловживань можуть швидко й надійно діагностувати використання конкретного інструментального засобу або технології атаки, це може допомогти адміністраторові скорегувати заходи для забезпечення безпеки;

детектори зловживань дозволяють адміністраторам, незалежно від рівня їхньої кваліфікації в області безпеки, почати процедури обробки інциденту.

Недоліки сигнатурного методу:

детектори зловживань можуть визначити тільки ті атаки, про які вони знають, необхідно постійно обновляти їхні бази даних для одержання сигнатур нових атак;

більшість детекторів зловживань розроблені таким чином, що можуть використовувати тільки строго певні сигнатури, а це не допускає визначення варіантів загальних атак.

Виявлення аномалій. Детектори аномалій визначають ненормальне (незвичайне) поводження на хості або в мережі. Вони припускають, що атаки відрізняються від "нормальної" (законної) діяльності і можуть бути визначені системою, що здатна відслідковувати ці відмінності. Детектори аномалій створюють профілі, що представляють собою нормальне поводження користувачів, хостів або мережних з'єднань. Ці профілі створюються, виходячи з даних історії, зібраних у період нормального функціонування. Потім детектори збирають дані про події й використовують різні метрики для визначення того, що аналізована діяльність відхиляється від нормальної.

Детектори аномалій і системи виявлення атак (СВА), що на них засновані, часто створюють велику кількість помилкових повідомлень, тому що зразки нормального поводження користувача або системи можуть бути дуже невизначеними. Незважаючи на цей недолік, вважається, що СВА, засновані на виявленні аномалій, мають можливість визначати нові форми атак, на відміну від СВА, заснованих на сигнатурах, які цілком покладаються на відповідність зразку минулих атак.

Переваги виявлення аномалій:

СВА, засновані на виявленні аномалій, фіксують несподіване поводження і, таким чином, мають можливість визначити симптоми атак без знання конкретних деталей атаки;

детектори аномалій можуть створювати інформацію, що надалі буде використовуватися для визначення сигнатур для детекторів зловживань;

притаманно виявляти кібератаки 0-day (атаки нульового дня). 0-day – вразливість програмного забезпечення, яка ще невідома користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту.

Недоліки виявлення аномалій:

виявлення аномалій звичайно створює велику кількість помилкових спрацьовувань про атаки при непередбаченому поводженні користувачів і непередбаченій мережній активності;

виявлення аномалій часто вимагає деякого етапу навчання системи, під час якого визначаються характеристики нормального поводження. Від якості проведення цього навчання суттєво залежить подальша ефективність СВА.

В таблиці 1 показано основне порівняння між методами виявлення зловживань та методами виявлення аномалії.

На основі аналізу розглянутих методів можна зробити висновок, що для підвищення рівня захищеності інформаційних ресурсів ІТС доцільно застосовувати методи на основі виявлення аномалій, оскільки саме їм притаманно виявляти кібератаки 0-day.

Основні засоби захисту від КА. До основних засобів захисту від КА відносяться: антивірусне програмне забезпечення; система запобігання/виявлення вторгнень IPS/IDS; мережеві екрани (Firewall). Типова схема застосування засобів захисту від КА представлена на рис. 1.

Таблиця 1

Порівняння між методами виявлення зловживань та методами виявлення аномалії

Особливість	**Методи виявлення ідентифікаторів**	
	Виявлення зловживань	**Виявлення аномалії**
Виявлені атаки	тільки відомі атаки	будь-якого типу
Необхідні фонові дані атаки	так	ні
Помилковий сигнал тривоги	низький	високий
Потреба в оновленні	так	ні
Тип атаки	визначений	не можна визначити
Ідентифікація інструменту захисту	так	ні

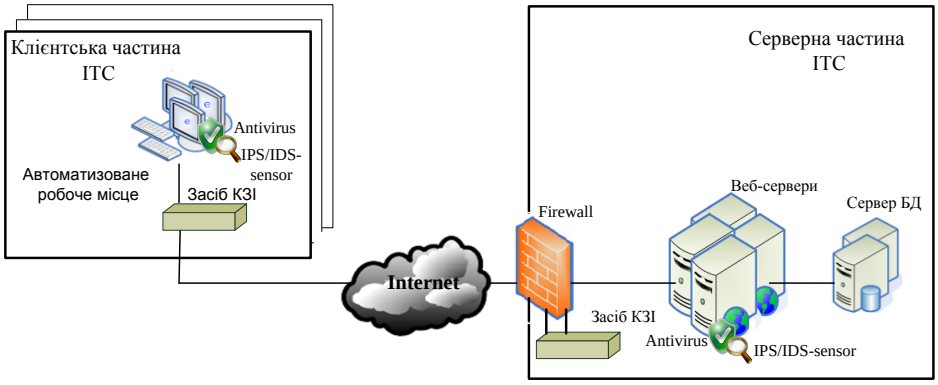

Рис. 1. Типова схема застосування засобів захисту від КА

Firewall (укр. мережевий екран) – це програма або обладнання, яке перешкоджає зловмисникам і деяким типам шкідливих програм віддалено отримувати доступ до ІТС. Для цього Firewall перевіряє дані, що надходять з Інтернету або по мережі, і розглядає їх на предмет блокування/дозволу передачі даних.

IDS/IPS – програмний та/або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою.

Антивірусний захист – програмне забезпечення, яке здатне інтерактивно знаходити, протидіяти, блокувати, а також повністю видаляти віруси з системи.

Розглянута типова схема їх застосування (рис. 1) має суттєвий недолік: всі засоби працюють окремо та мають свою досить вузьку область застосування.

Системи SIEM (Security information and event management) об'єднують управління інформаційною безпекою та управління подіями безпеки. Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків з метою покращення протидії КА. Цей підхід себе виправдовує, проте, включає весь спектр можливостей аналізованих засобів, що в свою чергу відображається на фінансовій складовій при покупці такої системи. В таблиці 2 показано порівняння лідерів ринку SIEM-систем: системи QRadar від IBM та ArcSight від HP.

Таблиця 2

Порівняльна таблиця SIEM-систем

Критерії	**IBM QRadar**	**HP ArcSight**
Передобробка лог-файлів	Виконується "на льоту"	Зберігає у сховище, а потім обробляє
Додавання конекторів	Розробка та додавання нових конекторів викликає складнощі	Гнучка система розробки та додавання конекторів
Кількість стандартних правил кореляції	Декілька сотень, розробка правил викликає труднощі	Декілька десятків, але має гнучкий механізм розробки правил
Автовизначення джерел подій	Розпізнавання джерела	Налаштування проводиться вручну

	відбувається автоматично	
Можливість моніторингу мережевого трафіку	Повний аналіз мережевого трафіку до 7 рівня	Аналіз мережевого трафіку до 4 рівня
Візуалізація зкорельованих подій	Надає інформацію про уразливість, порушника, топологію мережі	Констатує лише факт наявності події
Методи створення правил кореляції	На основі знань, обчислювального інтелекту, поведінкові	
Методи прийняття рішень	Поведінкові, на основі знань	

Тому пропонується до розглянутої схеми (рис. 1) додати координатор (рис. 2), основною метою якого буде координація дій всіх засобів з вузьким спектром всіх функцій. Координація функціонування цих засобів полягає в обміні командами управління та критичними даними в процесі аудиту подій в ІТС.

Наприклад, у випадку ідентифікації IDS/IPS мережевої кібератаки на основі наявної аномалії в системі, брандмауеру надається команда від координатора на блокування ір-адреси підозрілої активності на основі даних, отриманих від IDS/IPS. В іншому випадку при наявності підозрілої активності без чіткої ідентифікації атаки, координатор надає команду управління антивірусному програмному забезпеченню для відправлення даного процесу у карантин для подальшого дослідження.

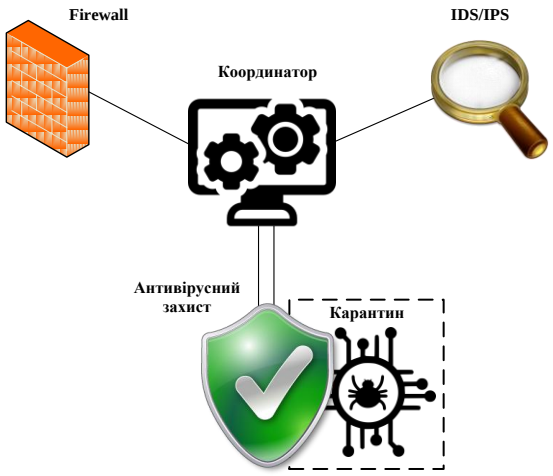

Рис. 2. Схема захисту від КА з використанням координатора

В умовах, коли керуюча система координатора не володіє повною інформацією про стан інформаційного середовища, обґрунтовується необхідність розробки моделі протидії загрозам, в якій існує можливість вибору того керуючого впливу, що найбільшою мірою відповідає стану координатора. Формулюються принципи розробки моделі протидії загрозам, наводиться формалізований опис методу прийняття рішень по вибору оптимального варіанта реагування на події безпеки.

Введемо певні визначення та терміни для формулювання моделі реагування на події в кіберсередовищі таким кортежем:

$$\{U_i, V_j, C(V_j), P_a, P(z_l), J, U^*(P_a)\},$$

де U_i – варіант реагування на події координатора; i – варіант реагування; V_j – результат реагування на події координатора; j – збиток; C_j – оцінка збитку координатора від атакуючої дії; z – параметр невизначеності стану середовища координатора; $P(z_l)$ – ймовірність стану середовища координатора; J – цільова функція вибору координатора; $U^*(P_a)$ – раціональний варіант реагування на події координатора; P_a – ймовірність атаки; l – номер сегмента.

Аналіз можливих варіантів реагування $\{U_i\}$ на події безпеки показав, що число керуючих впливів для кожної ситуації обмежене, $i \in$ [1, 3]. Оскільки вибір здійснюється в

умовах можливого здійснення атаки, пропонується пов'язувати систему переваг альтернатив з оцінкою збитку: *відсутність збитку, збитків одному користувачеві, збиток групі користувачів, збиток від реалізації атаки* ($\{V_j\}$, $j \in [1, 4]$). Задається функціонал [7 – 9], за яким здійснюється вибір оптимального варіанта реагування:

$$J(U_i, z)=\sum_{l=1}^{S} C_j(V_j(U_i, z_l))\, P(z_l),$$

де $P(z_l)=\prod_{i=1}^{I} p_{ij}(V_j(U_i), P_a)$,

ймовірності p_{ij} настання кожного j-го результату при виборі i-го варіанта реагування пропонується розраховувати як функції імовірності атак

$$p_{ij}= p_{ij}(V_j(U_i), P_a), \quad \forall i : \sum_j p_{ij}=1.$$

За таких обставин раціональний варіант реагування $U^*(P_a)$ може бути визначений зокрема з виразу:

$$U^*(P_a)=U(\arg \min_i (J(U_i, z))).$$

Модель вибору раціонального варіанта реагування на події порушення безпеки серед, наприклад, можливих трьох (блокування в реальному часі доступу до Web-серверу з IP-адрес, що генерують потік HTTP-запитів; відбраковування будь-якого трафіку, вихідна адреса якого не є одною з IP-адрес певної установи та переконфігурування на маршрутизаторах і міжмережевих екранах функцій антиспуфінга та антиDoS) з урахуванням припустимого збитку від різних проявів стороннього кібернетичного впливу (відсутність збитку, збитків одному користувачеві, збиток групі користувачів, збиток від реалізації атаки в ІТС) може бути подана у вигляді орієнтованого графа (рис. 3).

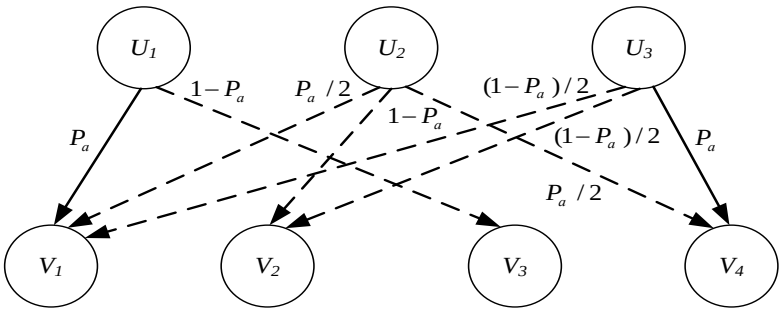

Рис. 3 Модель вибору раціонального варіанта реагування на події порушення безпеки

Варіанти реагування:

U_1 – блокування в реальному часі доступу до Web-серверу з IP-адрес, що генерують потік HTTP-запитів;

U_2 – відбраковування будь-якого трафіку, вихідна адреса якого не є одною з IP-адрес певної установи;

U_3 – переконфігурування на маршрутизаторах і міжмережевих екранах (в тому числі IDS/IPS та антивірусному захисті) функцій антиспуфінга та антиDoS.

Застосування такого підходу дозволить не тільки підвищити рівень кібернетичної захищеності ІТС, а й може бути платформою для автоматичного створення експлойтів та сигнатур кібератак на основі наявних аномалій. Вузький спектр всіх функцій координатора дозволить значно понизити фінансову складову в порівнянні з існуючими SIEM технологіями.

Висновки. Таким чином аналіз методів захисту від КА показав доцільність їх застосування до виявлення КА, але наразі не існує єдиного універсального методу захисту від всіх видів атак в ІТС. На основі аналізу розглянутих методів можна зробити висновок, що

для підвищення рівня захищеності інформаційних ресурсів ІТС доцільно застосовувати методи на основі виявлення аномалій, оскільки саме їм притаманно виявляти кібератаки 0-day.

Системи SIEM виправдовують себе, проте, включать весь спектр можливостей аналізованих засобів, що в свою чергу відображається на фінансовій складовій при покупці такої системи.

Запропонований у статті підхід передбачає включення до типової схеми застосування основних програмно та/або програмно-апаратних засобів захисту ІТС модуля-координатора, що дозволяє значно підвищити рівень захисту ІТС шляхом гібридизації їх функціоналу та зменшити вартість в порівнянні з існуючими SIEM технологіями за рахунок вузького спектру всіх функцій.

Подальшим напрямком наукових досліджень може бути вибір конкретного методу на основі виявлених аномалій та створення програмно-апаратних засобів захисту ІТС модуля-координатора.

ЛІТЕРАТУРА

1. Дрейс Ю.О., Мовчан М.С. Аналіз негативних наслідків кібератак на інформаційні ресурси об’єктів критичної інфраструктури держави, Актуальні питання забезпечення кібербезпеки та захисту інформації: третя міжнар. наук.-практ. конф., К.: Європейський університет, С. 71 – 74, 2017.

2. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. // Труды СПИИРАН. – 2016. – Вып. 47. С. 5 – 27 с.

3. Басараб М.А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов. // Вопросы кибербезопасности. – 2014. – № 4 (5). – С. 30 – 40.

4. Kumar, V. Parallel and distributed computing for cybersecurity / V. Kumar //IEEE Distributed Systems Online. – 2005. – Vol. 6, №. 10.

5. Браницкий А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко. // Труды СПИИРАН. – 2016. – № 45. – С. 207 – 244.

6. Feizollah, A. Anomaly Detection Using Cooperative Fuzzy Logic Controller / [A. Feizollah, S. Shamshirband, N. Anuar та ін.]. // Communications in Computer and Information Science. – 2013.

7. Котенко И.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак. /И.В. Котенко, М.В. Степашкин. // Труды ИСА РАН. Т. 31. – СПб., 2007. – С. 126 – 207.

8. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.

9. Машкина И.В. Управление и принятие решений в системах защиты информации: Учебн. пособие / И.В. Машкина. – Уфа: УГАТУ, 2007. – 160 с.