$$T_2 = E_1\left(1 - M_1\right) + \left(1 - E_1\right)E_2\left(1 - M_1\right)\left(1 - M_2\right) \quad (5)$$

Таким образом, вероятностная модель КС с двухуровневым стеком протоколов, представляющая собой выражение вероятностной функции оценки защищенности информации, обрабатываемой в КС, имеет вид:

$$P_2 = 1 - T_2 = \left(1 - E_1\right)\left(1 - E_2\right) + E_1 M_1 + \left(1 - E_1\right)E_2\left(M_1\left(1 - M_2\right) + M_2\right) \quad (6)$$

Аналогичное выражение, полученное для КС с N уровнями протоколов, для случая L угроз информации имеет следующий вид:

$$P(M) = \prod_{i=1}^{L}\left(\prod_{j=1}^{N}\left(1 - E_{ij}\right) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}\left(1 - E_{ik}\right)\cdot\left(\sum_{k=1}^{j} M_{ik}\cdot\prod_{l=k+1}^{j}\left(1 - M_{il}\right)\right)\right]\right) \quad (7)$$

где L – количество угроз информации, обрабатываемой в КС; N – количество уровней стека протоколов КС; M_{ij} – целочисленная переменная, значение которой определяет факт наличия/отсутствия механизма защиты от i-й угрозы на протоколе j-го уровня; E_{ij} – показатель эффективности реализации i-й угрозы на протоколе j-го уровня.

Выражение (7) представляет собой вероятностную модель защищенной КС с открытой архитектурой и произвольным количеством уровней стека протоколов, позволяющую оценить вероятность сохранения защищенности информации при воздействии на КС произвольного множества угроз. Данное выражение, совместно с ограничениями, заданными в виде (2), может быть использовано в качестве целевой функции (ЦФ), подлежащей максимизации путем решения соответствующей задачи математического программирования. В результате максимизации данной ЦФ может быть получено множество механизмов защиты $M=\{M_{ij}\}$, реализация которых в КС с открытой архитектурой обеспечит максимальную защищенность от множества угроз с эффективностями $E=\{E_{ij}\}$ при соблюдении заданных ограничений на суммарную стоимость включенных в состав СЗИ средств защиты, реализующих соответствующие механизмы.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. Гайкович В., Першин А. Безопасность электронных банковских систем.– М.: Изд-во компания "Единая Европа", 1993. 3. Federal Information Processing Standard (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June, 1974. 4. Рябинин И. А. Научная школа логико-вероятностных методов и концепция логико-вероятностной теории безопасности сложных систем // Теория и информационная технология моделирования безопасности сложных систем. Вып. 1 / Под ред. И. А. Рябинина. Препринт 101. СПб. ИПМАШ РАН, 1994. 5. Рябинин И. А. Концепция логико-вероятностной теории безопасности.– Приборы и системы управления, № 10, 1993.– с. 6–9. 6. Соложенцев Е. Д., Соложенцев В. Е. Моделирование поведения структурно-сложных систем: параметры, модели, знания, визуализация // Теория и информационная технология моделирования безопасности сложных систем. Вып. 2 / Под ред. И. А. Рябинина. Препринт 104. СПб. ИПМАШ РАН, 1994. 7. ISO 7498-2. Basic Reference Model – Part 2: Security Architecture. – February 1989. 8. IEEE802.10B. IEEE Standards for Interoperable Local Area Network (LAN) Security (SILS): Part B – Secure Date Exchange. – April 1992. 9. Рябинин И. А., Черкесов Г. Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. М.: Радио и связь, 1981.

УДК 681.3.06

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ И АУДИТА СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Виктор Кондратюк, Андрей Тимошенко
ООО «Институт компьютерных технологий»

Анотація: **Сформульовано основні вимоги і викладено принципи побудови систем централізованого контролю та аудиту засобів захисту корпоративної комп'ютерної мережі. Показано, як дані вимоги реалізовані в системі «Міраж».**
Summary: **The main ideas and principles of designing of centralized security monitoring and audit systems for corporate computer networks are formulated. The example of realization in a system «Mirage» is**

shown.
Ключові слова: **Спостережність, контроль, аудит, засоби захисту, корпоративна комп'ютерна мережа.**

В настоящее время в большинстве крупных предприятий развернуты корпоративные компьютерные сети (ККС), в составе которых, как правило, используются аппаратные и программные средства (устройства коммутации кадров сетевых протоколов, устройства маршрутизации пакетов сетевых протоколов, средства межсетевого экранирования, файловые серверы, серверы баз данных, серверы приложений, рабочие станции, операционные системы и т. п.) различных производителей.

Из особенностей современных ККС можно выделить следующее:

- распределенность;
- неоднородность с точки зрения входящих в состав ККС компонентов (файловые серверы, серверы приложений (HTTP, FTP и т. п.), серверы систем управления базами данных (СУБД), рабочие станции, активное сетевое оборудование – устройства маршрутизации, устройства коммутации и т. п.);
- неоднородность с точки зрения используемых операционных систем (ОС) и прикладных программных средств;
- реализация в большинстве используемых компонентов тех или иных стандартных (штатных) средств защиты, реализующих те или иные механизмы защиты информации (те или иные услуги безопасности);
- отсутствие единых средств управления средствами защиты и средств мониторинга и аудита функционирования средств защиты информации.

Уровень реализации в штатных средствах защиты компонентов ККС механизмов защиты информации во многих случаях является достаточным для того, чтобы использовать эти средства в составе комплексной системы защиты информации (КСЗИ), обрабатываемой в ККС предприятия.

Однако, согласно требованиям действующих в Украине нормативных документов (НД) в области технической защиты информации, важнейшей предпосылкой правильного построения КСЗИ является реализация в ней услуги наблюдаемости, позволяющей фиксировать деятельность пользователей и процессов, использование пассивных объектов ККС [3], а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и обеспечения ответственности за определенные действия. При этом, согласно требованиям НД [3], должна быть обеспечена возможность регистрации событий, имеющих непосредственное или косвенное отношение к безопасности, с фиксацией даты, времени, места, типа, успешности/неуспешности каждого зарегистрированного события. Зарегистрированная информация должна быть достаточной для установления пользователя, процесса и/или объекта, имевших отношение к каждому зарегистрированному событию, должна быть реализована возможность контроля единичных или повторяющихся событий, которые могут свидетельствовать о прямых нарушениях политики безопасности, принятой в ККС. Выявление и анализ несанкционированных действий должно выполняться в реальном времени с немедленным информированием администратора безопасности о превышении порогов безопасности.

К сожалению, эти требования не могут быть выполнены при помощи штатных средств защиты, реализованных в компонентах ККС. Данная услуга должна реализовываться путем создания надстроенной системы централизованного контроля и аудита средств защиты ККС.

Сравнительный анализ средств, представленных на рынке

В настоящее время на рынке СНГ представлен ряд продуктов, реализующих те или иные функции централизованного контроля и аудита средств защиты.

Данные средства делятся на два больших класса: средства мониторинга безопасности сетей, специально предназначенные для решения задач мониторинга и аудита средств защиты ККС и средства централизованного мониторинга и управления сетевыми ресурсами, в которых в качестве отдельных подсистем реализуются подсистемы мониторинга и аудита средств защиты.

Среди средств мониторинга безопасности сетей, представленных на рынке, можно выделить:

- **Intruder Alert** (производитель – Axent Technologies/Symantec Corporation, США);
- **RealSecure** (производитель – Internet Security Systems, США);
- **Secret Net 4.0** (производитель – НИП “Информзащита”, Россия);
- **Сова** (производитель – ООО «Анна», Украина);
- **Инспектор** (производитель – предприятие «Геос-Информ», Украина);
- **BackNET 2.0** (производитель – Государственный центр информационной безопасности, Украина).

В таблице 1 приведены результаты сравнительного анализа данных средств.

Таблица 1 – Результаты сравнительного анализа систем мониторинга безопасности компьютерных сетей

Название системы	Перечень контролируемых объектов ККС	Возможность мониторинга и аудита штатных средств защиты контролируемых объектов ККС	Протоколы взаимодействия с агентами на контролируемых объектах ККС	Возможность расширения перечня контролируемых объектов ККС
Intruder Alert	Серверы под управлением ОС WindowsNT/2000, Novell Netware, Unix-совместимых ОС, устройства маршрутизации, устройства коммутации	Да	Собственный, SNMP	Да (по протоколу SNMP)
RealSecure	Серверы под управлением ОС WindowsNT/2000, Unix-совместимых ОС, серверы СУБД	Да	Собственный	Нет
Secret Net 4.0	Серверы и PC под управлением ОС WindowsNT/2000	Да	Собственный	Нет
Сова	Серверы и PC под управлением ОС Windows95/98/NT/2000	Нет	Собственный	Нет
Инспектор	Серверы и PC под управлением ОС Windows95/98/NT/2000	Нет	Собственный	Нет
BackNET 2.0	Серверы под управлением ОС WindowsNT/2000, Unix-совместимых ОС, устройства маршрутизации, устройства коммутации	Нет	Собственный, SNMP, CCMNP	Да (по протоколам SNMP, CCMNP)

Среди представленных на рынке средств централизованного мониторинга и управления сетевыми ресурсами, в которых в качестве отдельных подсистем реализованы подсистемы мониторинга и аудита средств защиты, можно выделить следующие системы:

- **SPECTRUM** (производитель – компания Cabletron Systems, США);
- **HP OpenView** (производитель – компания Hewlett Packard, США);
- **Tivoli** (производитель – компания IBM, США).

Результаты сравнительного анализа данных средств приведены в таблице 2.

Таблица 2 – Результаты сравнительного анализа средств централизованного мониторинга и управления сетевыми ресурсами

Название системы	Перечень контролируемых объектов ККС	Возможность мониторинга и аудита штатных средств защиты контролируемых объектов ККС	Протоколы взаимодействия с агентами на контролируемых объектах ККС	Возможность расширения перечня контролируемых объектов ККС
SPECTRUM (Cabletron Systems, США)	Серверы под управлением ОС WindowsNT/2000, Unix-совместимых ОС, устройства маршрутизации, устройства коммутации	Только для устройств маршрутизации, и устройств коммутации	SNMP	Да (по протоколу SNMP)
HP OpenView (Hewlett Packard, США)	Серверы под управлением ОС WindowsNT/2000, Unix-совместимых ОС, устройства маршрутизации, устройства коммутации	Да	SNMP	Да (по протоколу SNMP)
Tivoli (IBM, США)	Серверы под управлением ОС WindowsNT/2000, Unix-совместимых ОС, устройства маршрутизации, устройства коммутации	Только для устройств маршрутизации, и устройств коммутации	SNMP	Да (по протоколу SNMP)

Анализ результатов, приведенных в таблицах 1 и 2, позволяет сделать вывод о том, что, во-первых, ни одна из представленных на рынке систем не обеспечивает возможность мониторинга и аудита средств защиты, реализованных во всех компонентах ККС, во-вторых, часть систем (**Сова, Инспектор, BackNET 2.0, SPECTRUM, Tivoli**) не обеспечивает возможность мониторинга и аудита штатных средств защиты ОС, а в-третьих, большая часть анализируемых систем мониторинга безопасности сетей являются закрытыми, не обеспечивающими возможность расширения перечня контролируемых объектов.

Обоснование требований к структуре и функциям системы централизованного контроля и аудита

С учетом изложенных выше особенностей ККС и предъявляемых нормативными документами требований к реализации услуги наблюдаемости можно сформулировать требования к функционированию системы централизованного контроля и аудита средств защиты ККС. Система должна обеспечивать:

- контроль и аудит штатных средств разграничения доступа ОС используемых в ККС серверов;
- контроль и аудит средств защиты используемых в ККС СУБД;
- контроль и аудит средств защиты используемых в ККС серверов приложений;
- контроль и аудит средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов;
- контроль и аудит средств разграничения доступа устройств коммутации кадров сетевых протоколов;
- анализ и обработку полученной информации в реальном времени с возможностью оперативного оповещения администратора о выявленных нарушениях политики безопасности.

На основании приведенных выше результатов сравнительного анализа представленных на рынке средств можно сформулировать следующие основные принципы построения системы централизованного контроля и аудита средств защиты ККС:

- система централизованного контроля и аудита средств защиты должна строиться по клиент-серверной архитектуре и включать в себя сервер безопасности (СБ), автоматизированное рабочее место администратора безопасности (АРМ АБ) и агентов системы централизованного контроля и аудита средств защиты, функционирующих на контролируемых объектах ККС;
- для обеспечения возможностей интеграции с другими средствами и расширения используемых методов обработки и анализа информации СБ должен обеспечивать возможность сохранения зарегистрированной информации в промышленной СУБД;
- СБ должен обеспечивать автоматическое (без вмешательства оператора) взаимодействие как с программными агентами, функционирующими на контролируемых объектах ККС, так и со стандартными syslog-, SNMP-агентами средств сетевого управления и мониторинга, реализованными в устройствах коммутации кадров и маршрутизации пакетов сетевых протоколов;
- в системе централизованного контроля и аудита средств защиты должна обеспечиваться возможность расширения перечня типов контролируемых системой объектов.

Реализация требований к системам централизованного контроля и аудита средств защиты корпоративной компьютерной сети

Сформулированные выше принципы построения систем централизованного контроля и аудита средств защиты ККС реализованы в системе «Мираж», разработанной ООО «Институт компьютерных технологий».

Система «Мираж» предназначена для реализации услуги наблюдаемости в КСЗИ, обрабатываемой в ККС предприятия, путем выполнения следующих функций:

- обеспечения контроля и аудита штатных средств разграничения доступа ОС;
- обеспечения контроля и аудита средств защиты СУБД;
- обеспечения контроля и аудита средств защиты серверов приложений (FTP, HTTP и т. п.);
- обеспечения контроля и аудита средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов, средств разграничения доступа устройств коммутации кадров сетевых протоколов, средств межсетевого экранирования и сенсоров систем обнаружения сетевых атак;
- анализа и обработки информации контроля и аудита, полученной от контролируемых объектов.

В терминах нормативного документа [3] входящие в состав системы «Мираж» средства реализуют функциональный профиль защищенности информации, включающий следующие функциональные услуги безопасности:

КВ-1 – минимальная конфиденциальность при обмене;

ЦВ-1 – минимальная целостность при обмене;

ДС-1 – устойчивость при ограниченных отказах;

ДЗ-1 – модернизация;
ДВ-1 – ручное восстановление;
НР-5 – анализ в реальном времени;
НИ-2 – одиночная идентификация и аутентификация;
НК-1 – однонаправленный достоверный канал;
НО-2 – разграничение обязанностей администратора;
НВ-2 – аутентификация источника данных;
НЦ-1 – КСЗ с контролем целостности;
НТ-2 – самотестирование при старте.
Функциональная схема и компоненты, входящие в состав системы «Мираж», представлены на рис. 1.

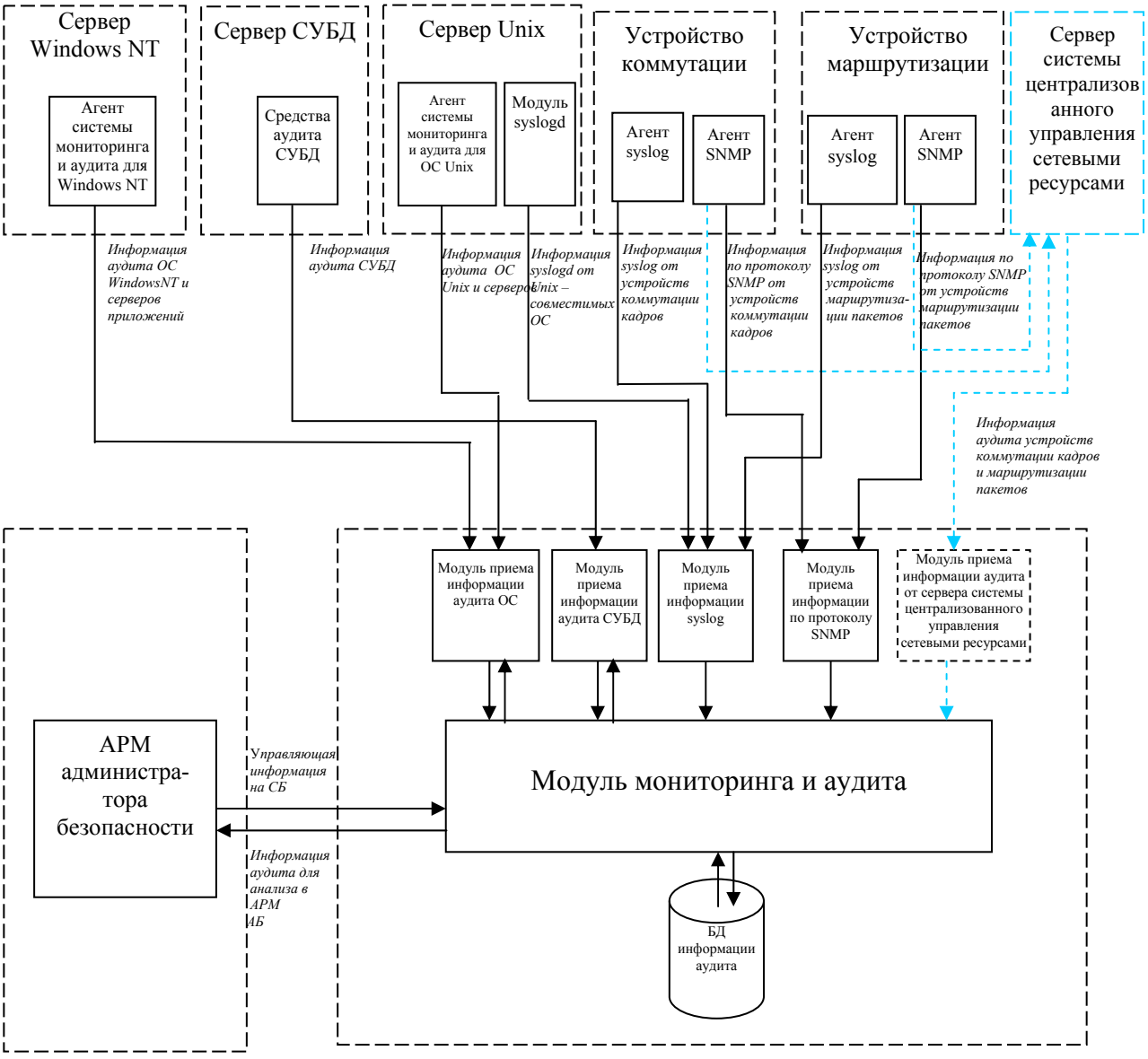

Рисунок 1 – Функциональная схема системы централизованного контроля и аудита средств защиты корпоративной компьютерной сети “Мираж”

СБ, на котором функционируют программные средства (ПС), осуществляющие выполнение функций мониторинга и аудита, а также ПС, обеспечивающие взаимодействие с агентами системы, функционирующими на контролируемых объектах, либо со стандартными средствами протоколирования, имеющими отношение к безопасности событий,

реализованными в ПС и ОС контролируемых объектов;

– агенты системы, функционирующие на контролируемых объектах (серверах) и взаимодействующие со стандартными средствами протоколирования, имеющими отношение к безопасности событий, реализованными в ОС контролируемых серверов;

– АРМ АБ, ПС которого обеспечивают возможность управления системой и анализа полученной информации.

Система централизованного контроля и аудита средств защиты ККС «Мираж» версии 1.01 обеспечивает:

– контроль и аудит средств разграничения доступа ОС Windows NT/2000;

– контроль и аудит стандартных средств разграничения доступа Unix-совместимых ОС по протоколу syslog;

– контроль и аудит расширенных средств разграничения доступа Unix-совместимых ОС;

– контроль и аудит средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов, средств разграничения доступа устройств коммутации кадров сетевых протоколов, средств межсетевого экранирования и сенсоров систем обнаружения сетевых атак по протоколу syslog;

– контроль и аудит средств разграничения доступа устройств маршрутизации пакетов сетевых протоколов, средств разграничения доступа устройств коммутации кадров сетевых протоколов, средств межсетевого экранирования и сенсоров систем обнаружения сетевых атак по протоколу SNMP;

– контроль и аудит средств разграничения доступа СУБД ORACLE, функционирующей на любой платформе.

Анализ информации, принятой от объектов контроля, выполняется на СБ в реальном времени. В случае обнаружения критичных для безопасности событий имеется возможность оперативного оповещения администратора безопасности (через консоль АРМ администратора, e-mail, sms и т. п.).

Модульная структура ПС СБ позволяет легко расширять его возможности (например, путем обеспечения мониторинга различных серверов приложений, устройств, поддерживающих протокол SNMP и т. п.).

В случае использования в ККС системы централизованного управления сетевыми ресурсами (типа HP OpenView, SPECTRUM и т. п.) информация, получаемая СБ от устройств коммутации кадров и маршрутизации пакетов сетевых протоколов (по протоколу SNMP), может быть получена с сервера данной системы.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 3. НД ТЗИ 2.5-004-99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа. 4. Баранов А. В., Петренко С. А. Системная интеграция и безопасность компьютерных сетей. Защита информации. Конфидент. № 2, 2001. 5. Внутренний мир Unix: Пер. с англ./ Хейр Крис и др. – К.: Издательство «ДиаСофт», 1998. 6. Доценко С. М. Система сетевой безопасности от одного производителя: миф или реальность? Безопасность информации, № 3, 2000. 7. Лукацкий А. В. Безопасность корпоративной сети глазами специалистов. Экспресс Электроника, № 4, 1999. 8. В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. Безопасность компьютерных сетей на основе Windows NT – М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd.", 1998. – 304 с. 9. Oracle8 Concepts. Release 8.0. A58277-01. 10. Real Secure. Network Sensor User Guide. Internet Security Systems, 2000. 11. Richard Power. Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare. Computer Security Institute, 1995. 12. Spectrum Concepts Guide. Cabletron Systems, 1996.

УДК 621.391.7

СУЧАСНИЙ СТАН РОЗВИТКУ КОНЦЕПЦІЇ ВІДВІДНОГО КАНАЛУ ТА ЗАДАЧІ ПОДАЛЬШОГО РОЗВИТКУ КОДОВОГО ЗАХИСТУ

Галина Кривоножко
ВІТІ НТУУ "КПІ"

Анотація: **Обговорюється проблематика та сучасний стан теорії кодового захисту інформації у спеціальних телекомунікаційних системах. Розглядаються найважливіші задачі аналізу та синтезу систем з кодовим захистом інформації. Обґрунтовуються показники і критерії стійкості цих систем.**