Дж. Обзор методов аутентификации информации // ТИИЭР. Т. 76.– 1988.– № 5.– С. 105–125. 5. Лужецький В. А., Яремчук Ю. Є. Рекурентні V_k –послідовності // Вісник ВПІ.– 1999.– № 6.– С. 53–59. 6. Лужецький В. А., Яремчук Ю. Є. Про один клас рекурентних послідовностей // Наукові праці Донецького державного технічного університету. Серія "Проблеми моделювання та автоматизації проектування динамічних систем".– 1999.– № 10.– С. 62–70. 7. Яремчук Ю. Є. Методи та засоби шифрування інформації на основі рекурентних послідовностей.– Дис. ... канд. техн. наук: 05.13.21 – К., 2000.– 179 с.

УДК 681.3.06

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА СЕМЕЙСТВА "ГРИФ"

Виктор Кондратюк, Дмитрий Корниенко
ООО «Институт компьютерных технологий»

Анотація: **Надано загальний опис можливостей комплексів засобів захисту від НСД родини "Гриф". Розглянуто проблеми оцінки таких комплексів на відповідність вимогам діючих в Україні критеріїв.**
Summary: **The brief description of functionality of unauthorized access protection systems from "Grif" family is given. Problems of such systems evaluation according to the Ukrainian criteria are discussed.**
Ключові слова: **Несанкціонований доступ, комплекс засобів захисту, критерії оцінки, криптографічний захист, централізоване керування.**

В статье рассмотрено две группы вопросов: во-первых, принципиальные отличительные функциональные характеристики прошедшей экспертную оценку первой версии комплекса средств защиты от несанкционированного доступа (КСЗ от НСД) "Гриф", которые выделяют его среди других аналогичных имеющихся на рынке систем; во-вторых, особенности второй версии КСЗ с централизованным удаленным администрированием. Ниже как синоним термина КСЗ иногда употребляется термин "система защиты".

Итак, краткая характеристика. Комплекс средств защиты от НСД "Гриф" предназначен для защиты обрабатываемой на ПЭВМ информации от несанкционированного ознакомления, модификации, удаления. КСЗ "Гриф" служит специализированной надстройкой над стандартной операционной системой (ОС) MS Windows 95/98 и дополняет ее функциями разграничения доступа. Комплекс позволяет создать защищенное автоматизированное рабочее место с ограниченным кругом пользователей, обладающих различными полномочиями по доступу к ресурсам.

Согласно выданному Департаментом специальных телекоммуникационных систем и защиты информации Службы безопасности Украины экспертному заключению (№ 10 от 18. 07. 2001 г.) совокупность реализованных в комплексе "Гриф" функций и механизмов защиты информации обеспечивает уровень защищенности информации, достаточный для обработки информации, составляющей государственную тайну.

КСЗ "Гриф" реализует следующие функции:

- *идентификацию и аутентификацию пользователей* при загрузке ПЭВМ до загрузки каких-либо программных средств с дисков на основании вводимого пароля и носимого идентификатора;
- *блокировку загрузки ОС с гибкого диска и CD-ROM*;
- *разграничение доступа пользователей к выбранным каталогам* и находящимся в них файлам;
- *управление потоками информации* и блокировку потоков информации, приводящих к снижению ее конфиденциальности;
- *гарантированное удаление конфиденциальной информации* путем затирания содержимого файлов при их удалении;
- *контроль за выводом информации на печать*;
- *контроль целостности прикладного программного обеспечения (ПО) и ПО КСЗ*, а также блокировку загрузки посторонних (незарегистрированных) программ и программ, целостность которых нарушена;
- *блокировку устройств интерфейса пользователя* (гашение экрана и блокировку клавиатуры и мыши) по выбранной комбинации клавиш или после определенного периода бездействия пользователя;

- *регистрацию событий* (загрузка ОС пользователем и завершение сеанса работы, попытки несанкционированного доступа, запуск программ, доступ к конфиденциальной информации и т. д.) в специальных журнальных файлах (ЖФ);
- *администрирование* (определение ресурсов, регистрацию пользователей, назначение прав доступа, обработку ЖФ и т. п.).

Реализуемые системой защиты услуги безопасности можно выразить через функциональный профиль. Согласно НД ТЗИ 2.5–004–99 "Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа" КСЗ от НСД "Гриф" реализует следующий функциональный профиль:

{ КА-2, КО-0, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2 }.

Разработка выполнена в соответствии с требованиями к уровню гарантий Г-3.

Для того, чтобы сделать обоснованные выводы о том, что позволяет система и подходит ли она для применения в конкретных условиях, необходимо, как минимум рассмотреть политику безопасности системы в целом и каждой из реализованных услуг.

Итак, какова политика безопасности, реализуемая КСЗ "Гриф"? Прежде всего, необходимо отметить два момента.

Во-первых, разграничение доступа пользователей к ресурсам осуществляется в соответствии с концепцией диспетчера доступа (reference monitor), рис. 1.

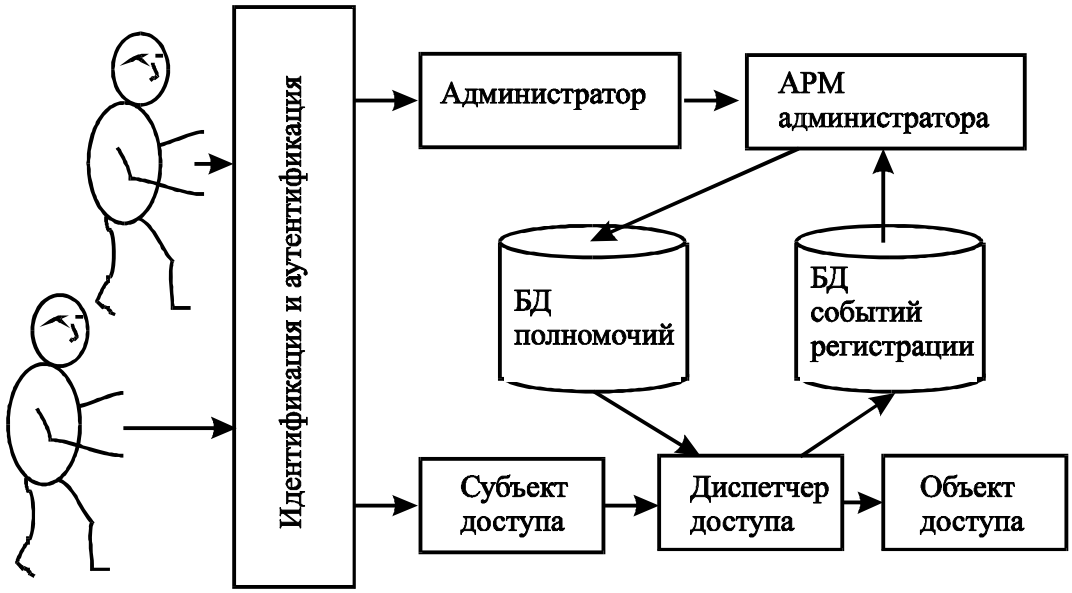

Рисунок 1 – Иллюстрация реализации концепции диспетчера доступа в КСЗ "Гриф"

В процессе проверки легальности каждого запроса на доступ к ресурсам участвуют следующие компоненты вычислительной системы:

- *Активный объект (субъект доступа)* – пользователь или порождаемый пользователем процесс (фактически - программа, у которой находится управление, и которая в настоящий момент времени является представителем пользователя в системе), который пытается получить доступ к определенной информации.
- *Пассивный объект (объект доступа)* – пассивный источник/приемник информации, к которому происходит обращение и который нуждается в защите.
- *База данных авторизации* (*полномочий)* – информация, определяющая права доступа пользователей и процессов к пассивным объектам (атрибуты доступа).
- *База данных регистрации* – записи о запросах и предоставлении доступа субъектов к объектам.
- *Диспетчер доступа* – средства, которые реализуют функции защиты и обеспечивают безопасность информации путем управления созданием активных и пассивных объектов, предоставления активным объектам доступа к пассивным в соответствии с информацией, содержащейся в БД полномочий, и регистрации событий (действий активных объектов) в БД регистрации, т. е. реализуют установленные правила разграничения доступа.

Во-вторых, в КСЗ "Гриф" реализовано административное (mandatory) разграничение доступа. Это означает, что управление БД полномочий (атрибутами доступа) и БД регистрации осуществляют только

имеющие соответствующие полномочия пользователи – администраторы. Обычные пользователи не могут изменять атрибуты доступа, а значит и предоставлять другим пользователям доступ к информации, с которой они работают, а также выполнять любые функции по управлению КСЗ.

Теперь перейдем непосредственно к реализованным услугам.

Идентификация и аутентификация пользователя (НИ-3 – множественная идентификация и аутентификация, НК-1 однонаправленный достоверный канал)

Прежде чем осуществлять разграничения доступа к ресурсам КСЗ должен опознать пользователя и блокировать доступ неавторизованных пользователей. Для этого при входе пользователя в систему выполняется его идентификация (опознание) и аутентификация (проверка результатов идентификации).

Идентификация пользователя выполняется на основании вводимого им с клавиатуры имени (псевдонима). Аутентификация пользователя выполняется на основании вводимого им с клавиатуры пароля и предъявляемого носимого идентификатора. В качестве носимого идентификатора может выступать ключевая дискета или идентификатор Touch Memory. Таким образом, реализована аутентификация пользователя одновременно по двум принципам: "обладаю чем-то" – носимый идентификатор и "знаю что-то" – пароль.

В случае, если предоставленная пользователем информация аутентификации не соответствует эталону, доступ в систему блокируется. Кроме того, КСЗ ведет контроль за истечением срока действия полномочий пользователя и его пароля, а также за соответствием дня недели и временного интервала, в который пользователь осуществляет вход в систему, тем, которые заданы администратором.

Достоверный канал взаимодействия пользователь – КСЗ обеспечивается путем реализации функций идентификации и аутентификации программами, “прошитыми” в микросхеме ПЗУ расширения BIOS, которая входит в состав КСЗ. Эти программы получают управление после включения питания или сброса компьютера до загрузки каких-либо программ с диска.

В КСЗ "Гриф" реализована также возможность блокировки устройств интерфейса пользователя (клавиатуры, мыши и монитора). Блокировка осуществляется либо пользователем с помощью определенной комбинации клавиш, либо КСЗ при бездействии пользователя в течении определенного периода времени. Для разблокирования компьютера пользователю необходимо предъявить свой носимый идентификатор и ввести пароль.

Контроль целостности КСЗ и самотестирование (НЦ-1 – КСЗ с контролем целостности, НТ-2 – самотестирование при старте)

Контроль целостности КСЗ заключается в проверке целостности ПО КСЗ при каждой загрузке системы. Кроме того, данные операции могут выполняться по желанию администратора с использованием программы администрирования. В случае обнаружения нарушения целостности пользователю выдается соответствующее сообщение и дальнейшая работа блокируется. В такой ситуации необходимо вмешательство администратора для восстановления целостности или переинсталляции КСЗ.

Одним из дополнительных требований для более высоких уровней услуги "целостность КСЗ" является обеспечение невозможности обхода средств защиты, что включает обеспечение непрерывной работы этих средств от момента включения питания. Для того, чтобы блокировать возможность загрузки ОС в отсутствие средств защиты, программы, “прошитые” в микросхеме ПЗУ, реализуют:

- блокировку загрузки ОС с дискеты и CD-ROM;
- блокировку клавиатуры до загрузки драйвера реального режима.

Кроме того, КСЗ "Гриф" реализует контроль целостности программного обеспечения. Реализация данной функции преследует несколько целей:

- во-первых, препятствует распространению вирусов, а значит нарушению целостности ОС, КСЗ и информации;
- во-вторых, позволяет избежать утечки информации за счет использования скрытых каналов, нарушения установленной технологии обработки информации, а также других действий, связанных с внедрением "троянских коней";
- в-третьих, позволяет создать условия, когда в системе работает только проверенное ПО, которое по определению не выполняет никаких действий, которые могли бы привести к отключению или преодолению средств защиты, что позволяет выполнить требования более высоких уровней услуги "целостность КСЗ".

Контроль целостности ПО заключается в проверке целостности исполняемых модулей при их загрузке. Загрузка модулей, которые не соответствуют хранящейся в БД КСЗ эталонной записи, блокируется. БД эталона ПО создается и модифицируется уполномоченным администратором.

Разграничение доступа к ресурсам (КА-2 – базовая административная конфиденциальность, ЦА-1 – минимальная административная целостность, КО-0 – минимальное повторное использование объектов)

Разграничение доступа пользователей к ресурсам осуществляется на уровне каталогов. Каждому каталогу ставится в соответствие специальный атрибут – уровень конфиденциальности, который аналогичен грифу при работе с ИсОД и ограничивает возможности пользователей по доступу к данному каталогу. Каждому пользователю ставиться в соответствие уровень допуска.

В КСЗ "Гриф" введено два уровня допуска пользователей и конфиденциальности каталогов. Уровень допуска пользователя должен быть явно задан администратором, в противном случае по умолчанию он не может получить доступ к ИсОД (защищенным каталогам). Уровень конфиденциальности каталога устанавливается при его создании и не может быть изменен. Незащищенные каталоги считаются по умолчанию открытыми (не имеющими уровня конфиденциальности) и доступ к ним разрешен всем пользователям.

КСЗ ведет БД защищенных каталогов, управлять которой могут имеющие соответствующие полномочия администраторы. Для каждого защищенного каталога администратор устанавливает список доступа, в котором перечислены пользователи, имеющие права доступа к данному каталогу и находящимся в нем файлам (и подкаталогам), и разрешенные для этих пользователей типы доступа (чтение или чтение/запись). Для того, чтобы пользователь мог получить доступ к защищенному каталогу, его уровень допуска должен быть не меньше, чем уровень конфиденциальности каталога. Пользователи имеют только те права доступа к защищенным каталогам, а значит и к находящейся в них ИсОД, которые явно определены администратором.

КСЗ "Гриф" поддерживает управление потоками информации: КСЗ следит за тем, чтобы не осуществлялось перемещение информации (например, копирование файлов) из защищенных каталогов в каталоги с меньшим уровнем конфиденциальности или открытые. Кроме того, администратор имеет возможность явно определить специальные каталоги импорта/экспорта (например, дисковод A:) и пользователей, которые имеют доступ к ним, а также осуществлять контроль за выводом информации на печать.

Дополнительно к перечисленным правилам реализованы определенные ограничения на доступ (по записи) к каталогу КСЗ и файлам настройки ОС.

При попытке пользователя получить запрещенный вид доступа (например, удалить файл в каталоге, к которому разрешен доступ только по чтению) в журнальном файле КСЗ регистрируется попытка НСД и, если для пользователя не установлен "мягкий" режим реагирования на попытки НСД, в котором осуществляется только регистрация НСД, – доступ блокируется.

Дополнительно к функциям непосредственного разграничения доступа в КСЗ реализована услуга "повторное использование объектов". В случае включения данной возможности при удалении файлов, находящихся в защищенных каталогах, осуществляется запись поверх содержащейся в файлах информации псевдослучайной двоичной последовательности (так называемый wiping). Дополнительно может затираться информация, содержащаяся в записи каталога данного файла – имя файла и его длина.

Регистрация действий пользователей (НР-2 – защищенный журнал)

КСЗ регистрирует попытки несанкционированного доступа в специальных ЖФ и, если для пользователя не установлен "мягкий" режим реагирования на попытки НСД, блокирует выполнение несанкционированных действий. Кроме того, в ЖФ регистрируются факты входа пользователя в систему, а также факты изменения состояния БД КСЗ (регистрация пользователей и ПО, изменение прав доступа к файлам и т. д.). Дополнительно для каждого пользователя может быть установлена необходимость регистрации фактов запуска программ, доступа к защищенным каталогам и обращений к обычным (общим) файлам и каталогам (открытие файлов для чтения и/или записи, создание, переименование, удаление файлов и каталогов, просмотр содержимого каталогов).

В каждой записи ЖФ фиксируется дата и время события, тип и атрибуты операции (например, открытие файла для чтения/записи), атрибуты процесса и пользователя, инициировавших событие, признак успешности завершения операции и в случае отказа – причина, а также другая информация.

Обработка ЖФ (просмотр сообщений, анализ статистики и т. д.) осуществляется имеющим соответствующие полномочия администратором и включает просмотр информации, содержащейся в ЖФ,

отбор интересующих записей при просмотре по диапазону параметров, группировку повторяющихся событий или задаваемых администратором стандартных последовательностей событий в семантически значимые составные события, печать ЖФ.

Разграничение обязанностей (НО-2 – разграничение обязанностей администраторов)

За каждым администратором могут быть закреплены привилегии на: просмотр ЖФ, регистрацию ПО, регистрацию пользователей, управление правами доступа к каталогам. Кроме того, явно выделена роль главного администратора, который имеет право назначать административные привилегии и устанавливать другие атрибуты для остальных администраторов, однако не имеет и не может иметь права на управление доступом к каталогам.

Восстановление после сбоев (ДВ-1 – ручное восстановление)

В КСЗ "Гриф" предусмотрена возможность восстановления работоспособности системы главным администратором после сбоев, приведших к нарушению целостности ПО или БД КСЗ, и в других подобных ситуациях.

Таким образом, установка на ПЭВМ комплекса "Гриф" позволяет обеспечить:

- невозможность неконтролируемого и несанкционированного ознакомления, копирования и восстановления информации;
- невозможность неконтролируемой и несанкционированной модификации и удаления информации;
- предоставление доступа к информации только при условии достоверного распознавания пользователей и с учетом полномочий, предоставленных согласно служебной необходимости;
- учет действий пользователей и регистрацию попыток нарушения установленного порядка доступа к информации, включая блокировку доступа к информации в случае выявления таких попыток, а также возможность осуществления контроля за доступом к информации со стороны уполномоченных лиц.

Конечно, защита локального компьютера – это хорошо, однако в большинстве случаев недостаточно. В большинстве организаций компьютеры объединены в сеть, поэтому, естественным развитием локального КСЗ является создание КСЗ с централизованным управлением.

Следующим представителем семейства "Гриф" является КСЗ от НСД "Гриф-2", в котором реализовано централизованное удаленное администрирование локальных комплексов, установленных на рабочих станциях локальной или распределенной вычислительной сети с протоколом TCP/IP.

В КСЗ "Гриф-2" входит автоматизированное рабочее место удаленного администрирования (АРМ УА) и комплекс средств защиты рабочих станций (РС).

КСЗ "Гриф-2" на РС реализует следующие дополнительные по сравнению с КСЗ "Гриф" функции:

- криптографическую защиту файлов в выбранных каталогах в прозрачном режиме (на лету);
- поддержку удаленного администрирования.

Криптографическая защита

При установке защиты на каталог по желанию администратора может осуществляться зашифрование информации во всех файлах данного каталога и его подкаталогов. Шифрование информации осуществляется в соответствии с алгоритмом криптографической защиты, установленным ГОСТ 28147-89. После установки защиты расшифрование/зашифрование информации, находящейся в зашифрованных файлах, осуществляется в прозрачном режиме (на лету), т. е. непосредственно при чтении/записи информации в/из ОЗУ.

За счет реализации данной функции предотвращаются угрозы нарушения конфиденциальности защищенной информации в случае "обхода" средств защиты или отторжения носителей информации (НЖМД), например кражи. Кроме того, использование криптографических преобразований позволяет удовлетворить требования "Критериев" к услуге "повторное использование объектов" по отношению к файлам, находящимся в зашифрованных каталогах, даже без реализации затирания информации при удалении.

Удаленное администрирование

Для поддержки возможности удаленного администрирования в состав ПО КСЗ на РС вводится специальный компонент – агент АРМ УА (рис. 2.).

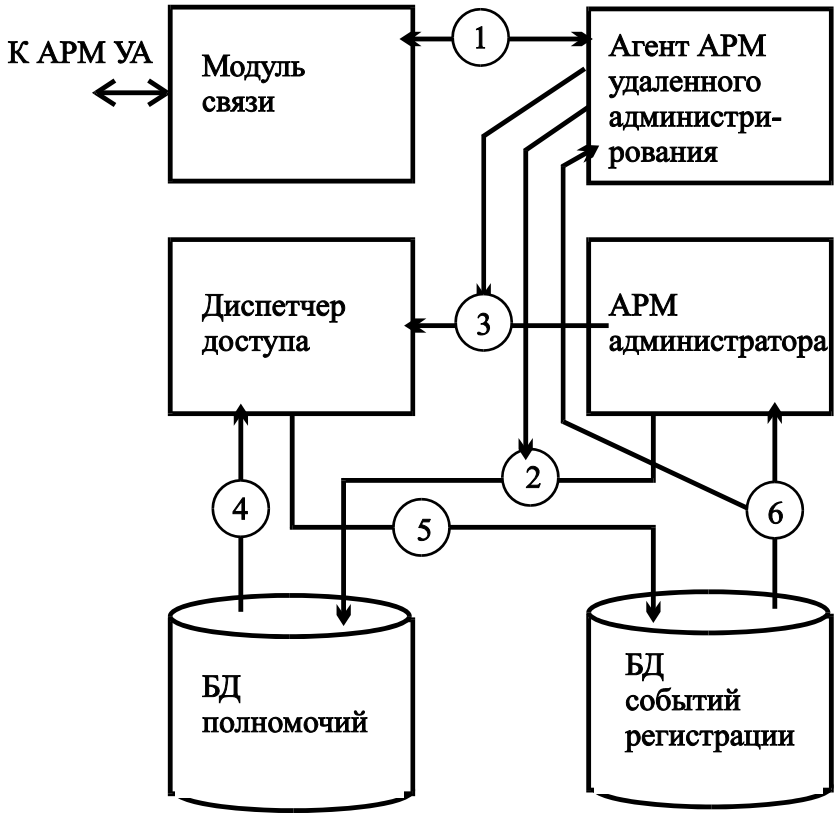

Рисунок 2 – Архитектура ПС КСЗ "Гриф-2" на РС

1) запросы/ответы от/к АРМ УА; 2) назначение прав доступа и полномочий; 3) управляющие воздействия к ДД; 4) проверка прав доступа; 5) регистрация событий; 6) просмотр журналов аудита.

Агент АРМ УА обеспечивает выполнение следующих функций:

- прием управляющих воздействий от АРМ УА;
- модификацию локальных БД в соответствии с управляющими воздействиями АРМ УА и выдачу управляющих запросов диспетчеру доступа;
- передачу модифицированных БД и ЖФ на АРМ УА;
- протоколирование запросов АРМ УА и действий по выполнению этих запросов.

АРМ УА реализует следующие функции:

- ведение централизованной БД РС (создание, удаление и модификацию атрибутов РС и групп РС);
- формирование паспорта РС в виде файла, необходимого для инсталляции РС;
- прием БД от РС и их просмотр;
- получение ЖФ от РС и их анализ;
- блокировку доступа пользователя к РС и предоставление такого доступа;
- передачу на РС управляющих воздействий, вызванных модификацией атрибутов РС или блокировкой/разрешением доступа пользователя к РС;
- идентификацию и аутентификацию пользователя АРМ УА;
- разграничение обязанностей администраторов системы "Гриф";
- настройку АРМ УА при помощи интерфейса пользователя АРМ УА.

Особое внимание при разработке было уделено синхронизации состояния локальных БД на РС и централизованой БД на АРМ УА, а также вопросам обеспечения защищенного канала обмена между АРМ УА и его агентами на РС с целью защиты передаваемой информации от несанкционированной модификации и просмотра.

КСЗ "Гриф-2" позволяет создать безопасную технологическую среду для систем электронного документооборота, банковских и других систем, для которых ключевым требованием является соблюдение конфиденциальности обрабатываемой информации и технологии ее обработки.

УДК 691.321

ПІДХОДИ ДО ВИЗНАЧЕННЯ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Геннадій Гулак, Людмила Ковальчук
ДСТСЗІ

Анотація: **Приводяться та порівнюються різні означення випадкових та псевдовипадкових послідовностей. Розглядається питання про тестування послідовностей.**
Summary: **Different definitions of random and pseudorandom sequences are compared. Question about testing of sequences is considered. Random and pseudorandom sequences, testing.**
Ключові слова: **Випадкові та псевдовипадкові послідовності, тестування.**

I Вступ

На практиці часто виникають два тісно пов'язаних між собою питання. Перше: як за поліноміальний час отримати послідовність чисел, що має певний набір властивостей, достатній для того, щоб її можна було вважати *випадковою*, тобто отриманою як *реалізацію послідовності незалежних випадкових величин з рівномірним розподілом,* що приймають значення у певному алфавіті? І друге питання: як визначити, чи можна деяку фіксовану послідовність вважати випадковою? У роботі розглядається декілька варіантів відповідей на ці запитання.

II Основна частина

§1. Визначення випадкової послідовності

Надалі ми розглядатимемо лише випадкові величини з дискретним розподілом, тобто для всіх *t* випадкові величини x_t приймають значення на множині $D = \{0, 1, ..., N-1\}$, що називається алфавітом послідовності.

За найбільш поширеним визначенням дискретна випадкова послідовність (РРВП) $\{x_t\}_{t\geq 1}$ – це послідовність незалежних (у сукупності) випадкових величин з рівномірним розподілом, тобто: $P(x_t = i) = N^{-1}$, де N називається об'ємом алфавіту D.

Випадкова послідовність має наступні властивості [11]:

1. $M(x_t) = 0.5 \cdot (N-1); \quad D(x_t) = 12^{-1} \cdot (N^2 - 1);$
2. $\forall k, \ \forall t_1, ..., t_k : \ P\{x_{t_1}, ..., x_{t_k}\} = N^{-k}$, тобто будь-який *k*-вимірний вектор з компонентами x_t має рівномірний на D^k розподіл.
3. будь-яка підпослідовність послідовності $\{x_t\}_{t\geq 1}$ також є РРВП;
4. сума за модулем *N* РРВП та будь-якої іншої послідовності, що від неї не залежить, також є РРВП;
5. РРВП не передбачувана, тобто для будь-якого натурального *n* кількість інформації по Шеннону, що міститься в $X_n = (x_1, ..., x_n)$ про майбутній елемент x_{n+1} дорівнює нулю: $I(x_{n+1}, X_n) = 0$.

Пристрій, що реалізує РРВП, називається *генератором* РРВП. Саме реалізації РРВП є тими об'єктами, що цікавлять нас. Одна з задач криптографії, що часто виникає на практиці, полягає у тому, щоб за конкретною реалізацією визначити, чи буде вона реалізацією РРВП. Для цього, зокрема, використовуються перелічені вище властивості РРВП та деякі інші її властивості. Надалі, для стислості викладу, реалізацію РРВП ми будемо називати просто випадковою послідовністю.

Існує багато визначень випадкової послідовності, але за різними причинами в своїй більшості вони не можуть бути застосовані на практиці.

Перший підхід до визначення випадкової послідовності був запропонований Шенноном та базується на теорії інформації [1]. Послідовність називається *випадковою за Шенноном*, якщо вміст інформації у ній