**ЗАНЯТТЯ 2.**

**ТЕМА: Вивчення досвіду побудови елементів КСЗІ. Методика побудови моделі комплексної оцінки загроз ОІД (держави агресора).**

**RU: Методика построения модели комплексной**

**оценки угроз информации, циркулирующей на**

**объекте информатизации**

Повышение эффективности **систем защиты информации (СЗИ)** **объектов информатизации (ОИ)** вызывает необходимость разработки и практического применения методического обеспечения, затрагивающего вопросы комплексной оценки угроз безопасности информации, анализа информационных рисков, оценки уровня защищенности ОИ.

Одним из первых этапов разработки СЗИ является анализ потенциально возможных угроз информации, хранимой, обрабатываемой и передаваемой по каналам связи на ОИ, при этом необходимо составить как можно более полную их совокупность и разработать модель угроз ОИ.

На основе изучения различных подходов к классификации угроз [1,2,3], в настоящей работе предпринята попытка возможно более полного анализа угроз безопасности информации.

При анализе угроз в первую очередь *выявляются источники угроз*, которыми могут быть:

- проектировщики и изготовители программно-аппаратных средств;

- внешний злоумышленник, осуществляющий проникновение в информационную среду ОИ через модем, широкополосный модем или беспроводную точку доступа;

- пользователь данного сегмента сети, соседнего сегмента или удаленный пользователь, осуществляющий воздействие на защищаемую информацию с нарушением прав и правил (нарушитель).

Далее *выявляются собственно угрозы* конфиденциальности, целостности, доступности. Причем в работе предлагается рассматривать множество угроз как множество каналов несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду ОИ (НСДУВ). При этом каждый канал НСДУВ рассматривается с одной стороны на множестве элементов угроз, с другой - на множестве элементов среды распространения носителя информации. Под элементом угрозы понимается потенциально возможное действие, совершаемое злоумышленником (нарушителем).

Нарушение информационной безопасности тогда можно рассматривать как последовательно реализуемые элементы угроз, что в итоге может привести к нанесению ущерба.

Такой подход позволяет оценить *вероятности осуществления угроз* злоумышленником (нарушителем) как вероятности реализации каналов НСДУВ.

Подход к рассмотрению «компьютерной угрозы» как виртуального технического канала получения информации сформулирован в [2].

В данной работе каналом НСД УВ (**несанкционированного доступа**, **утечки** информации или деструктивных **воздействий** на информационную среду отдельного **персонального компьютера** или сервера (**НСД УВ ПК**) и объекта информатизации в целом (**НСД УВ ОИ**)

считается путь распространения носителя информации при манипулировании злоумышленника (нарушителя) информационными потоками с целью достижения определенного воздействия на информационную среду ОИ. Простейшая структура канала НСДУВ содержит: ПК или другую аппаратуру злоумышленника, среду распространения носителя информации, информационную среду ОИ. Функционирование канала осуществляется как действие или последовательность действий (элементов угроз) злоумышленника(нарушителя) по манипулированию информационными потоками на множестве элементов физической среды распространения носителя.

Составив список таких потенциально возможных действий (элементов угроз), получим:

- попытка проникновения злоумышленника с подключением к среде распространения носителя информации;

- посылка ложных заявок на обработку;

- фильтрация информации идентификации и аутентификации;

- поиск точек входа в информационную среду ОИ или ПК последовательным перебором известных уязвимостей;

- сборка мусора на диске и в оперативной памяти;

- внедрение мобильных вредоносных кодов и программ;

- несанкционированный доступ к наборам данных;

- изменение базы данных защиты (настроек СЗИ) с последующим несанкционированным получением и использованием прав доступа;

- криптоанализ.

Такой подход позволяет разработать модели каналов **несанкционированного доступа**, **утечки** информации или деструктивных **воздействий** на информационную среду отдельного **персонального компьютера** или сервера (**НСД УВ ПК**) и объекта информатизации в целом (**НСД УВ ОИ**).

При разработке модели НСД УВ ПК используется структура типового ПК в виде:

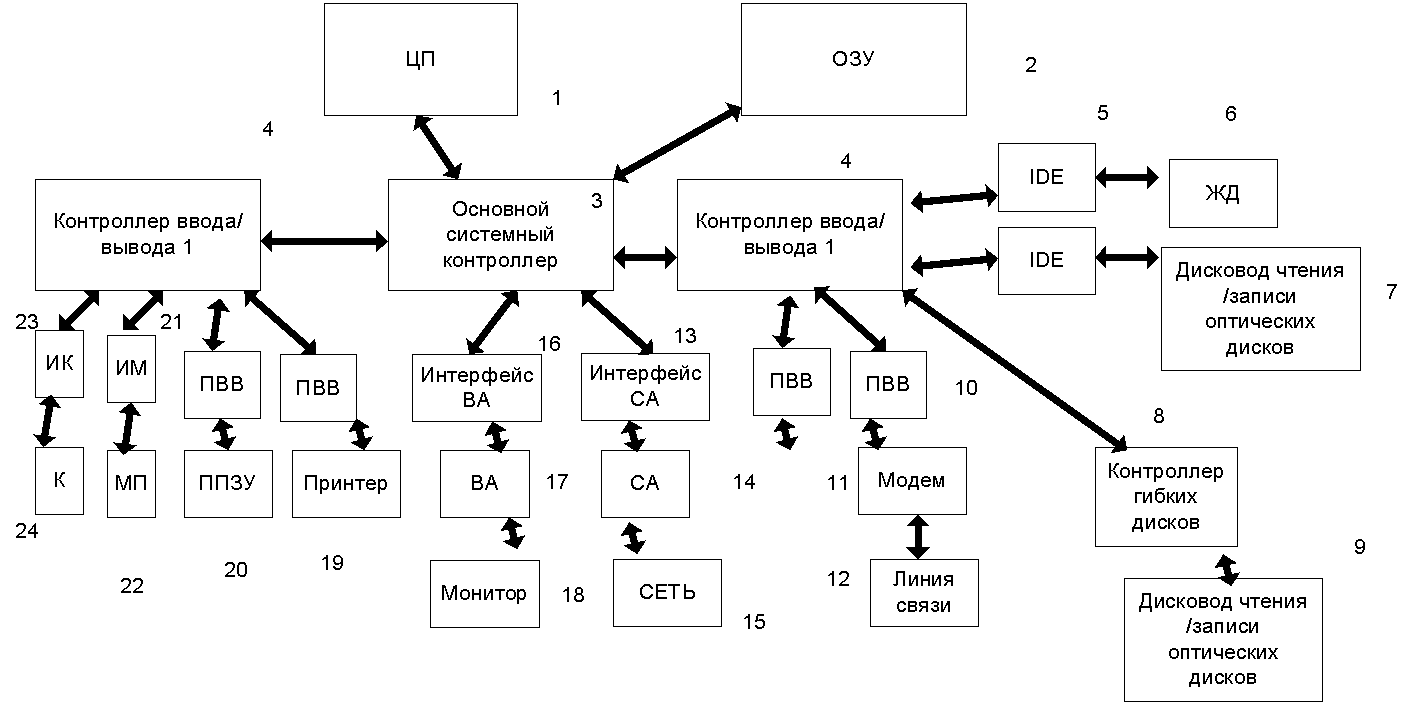


Рис. 1 Структура типового ПК

В соответствии со структурой рассматриваются:

* потенциально возможные действия злоумышленника и несанкционированные действия удаленного пользователя (использование скоростного канала через сетевой адаптер, менее скоростного канала через модем и дистанционный перехват излучений ПК злоумышленником);
* угрозы в случае прямого доступа нарушителя к ПК через его внешние разъемы (копирование информации с жесткого диска на различные носители информации, загрузка с различных носителей информации, внедрение вредоносных программ с носителей информации);
* угрозы в случае прямого доступа к ПК с возможностью его вскрытия (подключение жесткого диска к оборудованию нарушителя, внедрение закладных устройств).

Принят перечень типовых средств защиты и контроля защищенности ПК: система разграничения доступа (СРД), подсистема мониторинга и регистрации изменений (ПМРИ), антивирусная система (АС), система резервирования (СР), система шифрования (СШ), система обнаружения аномалий (СОА), средства защиты от ПЭМИ – электромагнитный экран (ЭМЭ).

Для каждого вида канала построены модели в виде графов структуризации каналов НСД УВ ПК, отображающие физический путь распространения носителя информации на множестве элементов структуры ПК с учетом взаимодействия угроз со средствами защиты на ПК. Пример такой модели для случая удаленного доступа злоумышленника (нарушителя) к информационной среде ПК через сетевой адаптер с целью нарушения целостности приведен на рисунке 2.

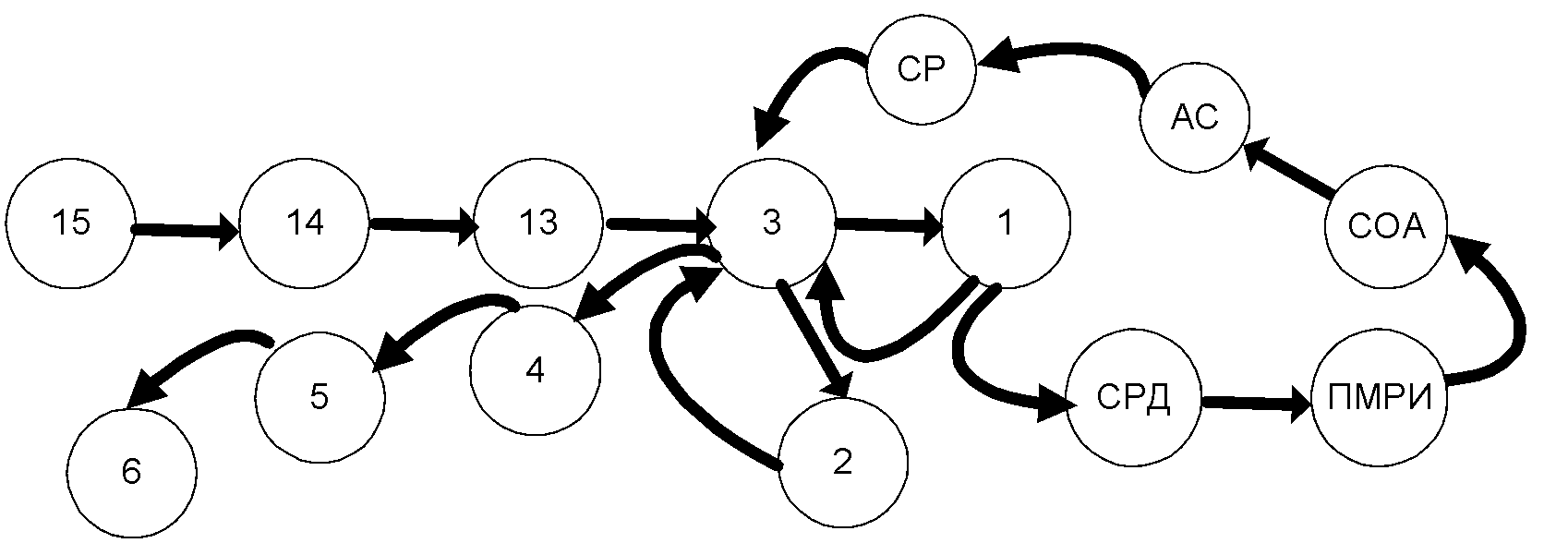


Рис. 2 Модель удаленного доступа злоумышленника /нарушителя к информационной среде ПК через сетевой адаптер с целью нарушения целостности.

По этой модели можно оценить вероятность реализации угрозы как произведение вероятностей успешного преодоления злоумышленником (нарушителем) защитных барьеров. Так для приведенного примера:

Pзуцел=Pзcрд\*( Pзпмр +(1-Pзпмр)\*Pзсоа)\*Pас\* Pср , (1)

где Pзуцел – расчетная вероятность нарушения целостности информации злоумышленником;

Pзcрд- вероятность преодоления системы разграничения доступа злоумышленником;

Pзпмр – вероятность необнаружения действий злоумышленника подсистемой мониторинга и регистрации;

Pзсоа – вероятность преодоления системы обнаружения аномалий;

Pср – вероятность отсутствия резервной копии;

Pас – вероятность преодоления системы антивирусной защиты.

На основе анализа всех потенциально возможных сценариев действий злоумышленника (нарушителя) разработана структурная вербальная модель каналов НСД УВ на информационную структуру ПК, представленная в следующей табличной форме:

Таблица 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вариант нарушения/канал НСД УВ | Цель воздействия | Структура канала на множестве элементов ПК и барьеров | Элемент воздействия или источник информации, источник опасного сигнала | Местонахождение источника информации или элемента воздействия или источника опасного сигнала | Вероятность реализации | Скорость канала | Время доступа | Производительность канала |
| **Удаленный доступ** |  |  |  |  |  |  |  |  |
| **1а) С подключением к сети** |  |  |  |  |  |  |  |  |
| **1б) Съем ПЭМИ** |  |  |  |  |  |  |  |  |
| **Прямой доступ к ПК** |  |  |  |  |  |  |  |  |
| **Прямой доступ к компьютеру со взломом** |  |  |  |  |  |  |  |  |

Далее рассматриваются все потенциально возможные каналы НСД УВ ОИ в целом на множестве элементов типовой структуры сети, частью которой (расположенной в помещениях одного здания) является объект информатизации. Введем следующие обозначения элементов структуры сети и средств защиты: рабочая станция (РС), файл-сервер (ФС), межсетевой экран, широкополосный модем (ШМ), беспроводная точка доступа (БТД), маршрутизатор (МР), линия связи (ЛС), switch (SW).

Построены модели в виде графов структуризации каналов НСД УВ в случае несанкционированных действий нарушителя из соседнего сегмента, из филиала организации, использующего модемный пул, беспроводную точку доступа при реализации угроз, состоящих из элементов описанных выше. Используя представление каналов в виде графов, можно оценить вероятности их реализации.

Пример модели канала НСДУВ ОИ при поиске нарушителем точек входа последовательным перебором уязвимостей через модем с использованием модемного пула приведен на рис. 3 на множестве элементов среды распространения носителя информации.

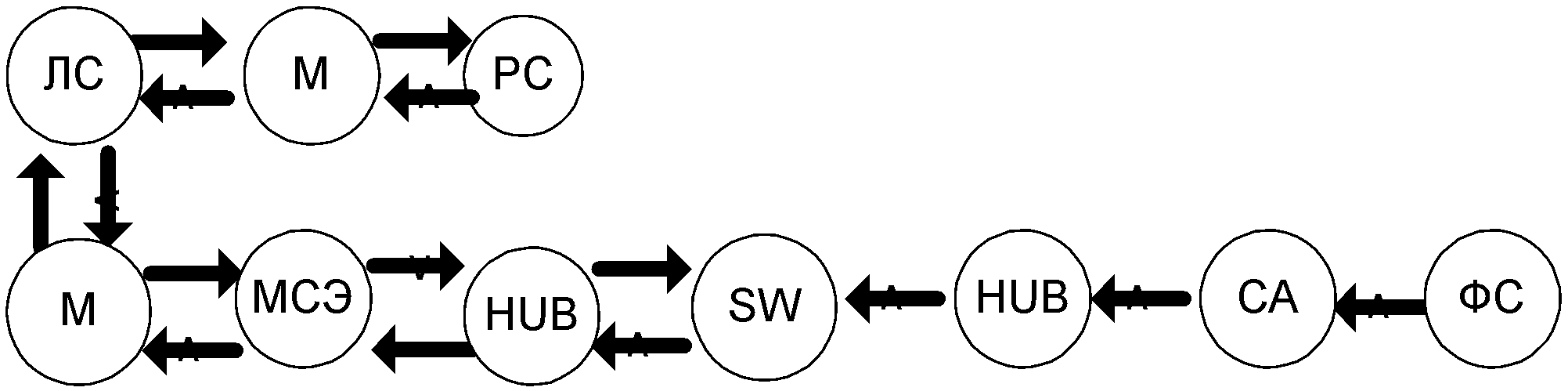


Рис. 3 Модель канала утечки информации при перехвате информации нарушителем через модем с использованием модемного пула

Pнпи3= Psw \*Pнш

где Pнпи3 – расчетная вероятность перехвата информации нарушителем через модем с использованием модемного пула;

Psw – вероятность преодоления нарушителем защиты свитча;

Pнш – вероятность преодоления нарушителем защиты трафика средствами шифрования.

Построены модели в виде графов структуризации аналогичных каналов НСД УВ ОИ, реализуемых злоумышленником.

Злоумышленнику первоначально необходимо осуществить этап подключения к среде распространения носителя информации. Попытка проникновения с подключением к среде распространения носителя по своему содержанию аналогична поиску точек входа последовательным перебором уязвимостей, и является характерной для злоумышленника. На этом этапе происходит сканирование злоумышленником периметра ОИ с целью обнаружения уязвимостей, эксплуатация которых позволяет ему проникнуть в сеть

Вероятность успешного выполнения этого этапа зависит от используемых средств защиты периметра сети.

Пример модели канала воздействия злоумышленника на ОИ, приводящего к нарушению доступности при посылке ложных заявок, через беспроводной адаптер с использованием точки беспроводного доступа, показан на рис . 4.

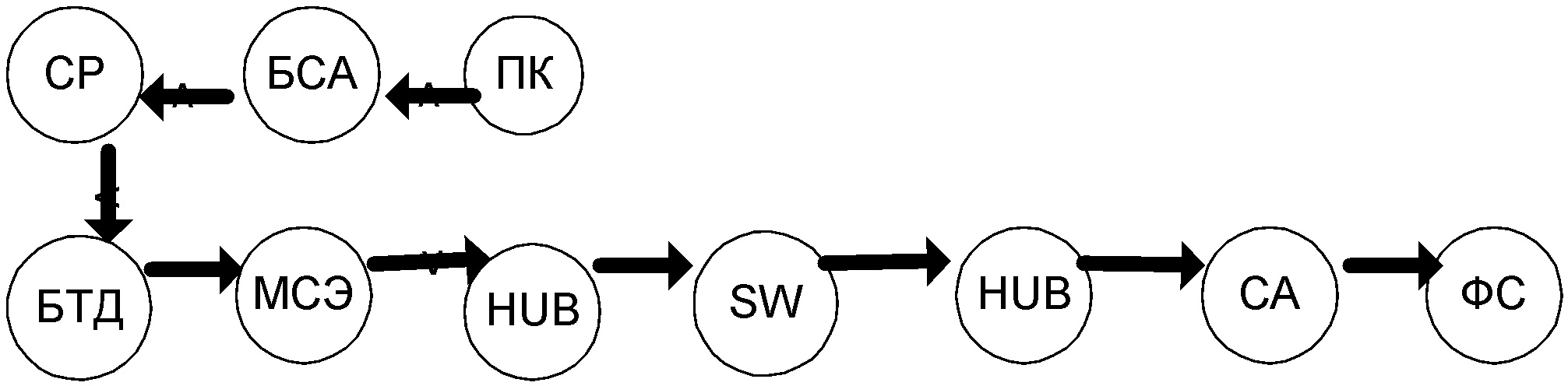


Рис. 4 Модель канала деструктивного воздействия злоумышленника на ОИ, приводящего к нарушению доступности при посылке ложных заявок через беспроводной адаптер с использованием точки беспроводного доступа

Вероятность этого этапа определяется как:

Pзлз3= Pзм \*Pзуд, где

Pзлз3– расчетная вероятность нарушения доступности посылкой ложных заявок через беспроводной адаптер с использованием точки беспроводного доступа;

Pзм – вероятность преодоления ложными заявками межсетевого экрана;

Pзуд – вероятность успешного преодоления злоумышленником средств защиты от блокирования доступа на файл-сервере.

На основе анализа потенциально возможных каналов НСД УВ ОИ, реализуемых злоумышленником (нарушителем), разработана структурная вербальная модель каналов НСД УВ ОИ, приведенная далее в табличной форме:

Таблица 2.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Канал / совокупность элементов угроз | Цель воздействия | Структура канала | Элемент воздействия или источник информации, источник опасного сигнала | Вероятность реализации канала | Местонахождение источника информации или элемента воздействия или источника опасного сигнала |
| Каналы, реализуемые злоумышленником | | | | | |
|  |  |  |  |  |  |
| Каналы, реализуемые нарушителем | | | | | |

Наиболее сложным этапом при построении моделей НСД УВ ПК и ОИ в целом является оценка вероятностей реализации каналов НСД УВ. В работе предлагается оценивать вероятность реализации каждого канала как произведение вероятностей элементов угрозы; при этом вероятности элементов угроз могут быть определены следующим образом:

* как статистические вероятности и вероятности, вычисленные на основе известной статистики (Pст Є[0,1]);
* методом нечеткой логики (Pнл Є[0,1]);
* если для выполнения элементарной угрозы необходимо преодоление существующего в системе барьера, то вероятность элемента угрозы принимается равной вероятности успешного преодоление злоумышленником (нарушителем) существующего барьера (PБ Є[0,1]).

Каждая из вероятностей элементарных угроз принадлежит одному из трех множеств: {Pст},{Pнл},{PБ}.

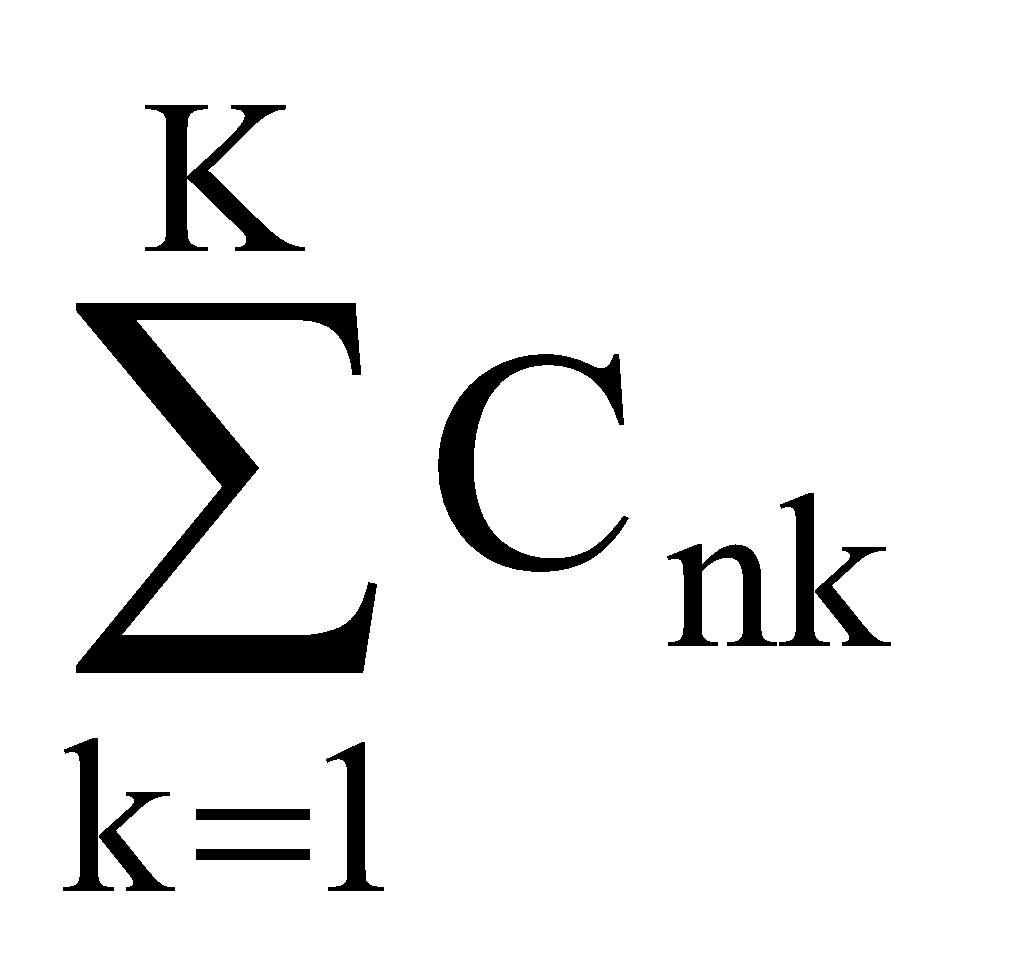
Таким образом, результирующие вероятности каналов НСДУВ, позволяют учесть динамику статистических значений элементов угроз, вероятности, полученные экспертным путем, и изменение вероятностей преодоления барьеров при замене средств защиты в случае модернизации СЗИ или при плановом управлении защитой информации.

Используя расчетные значения вероятностей реализации каналов НСД УВ, можно оценить, насколько адекватны реализованные в СЗИ механизмы и средства защиты информации существующим рискам; оценить уровень защищенности ОИ и определить, является ли он достаточным, какими мерами можно реально повысить уровень защищенности.

Методика расчета уровня защищенности информации на ОИ, основанная на ранее разработанной модели ОИ [4] и предложенной методике моделирования угроз.

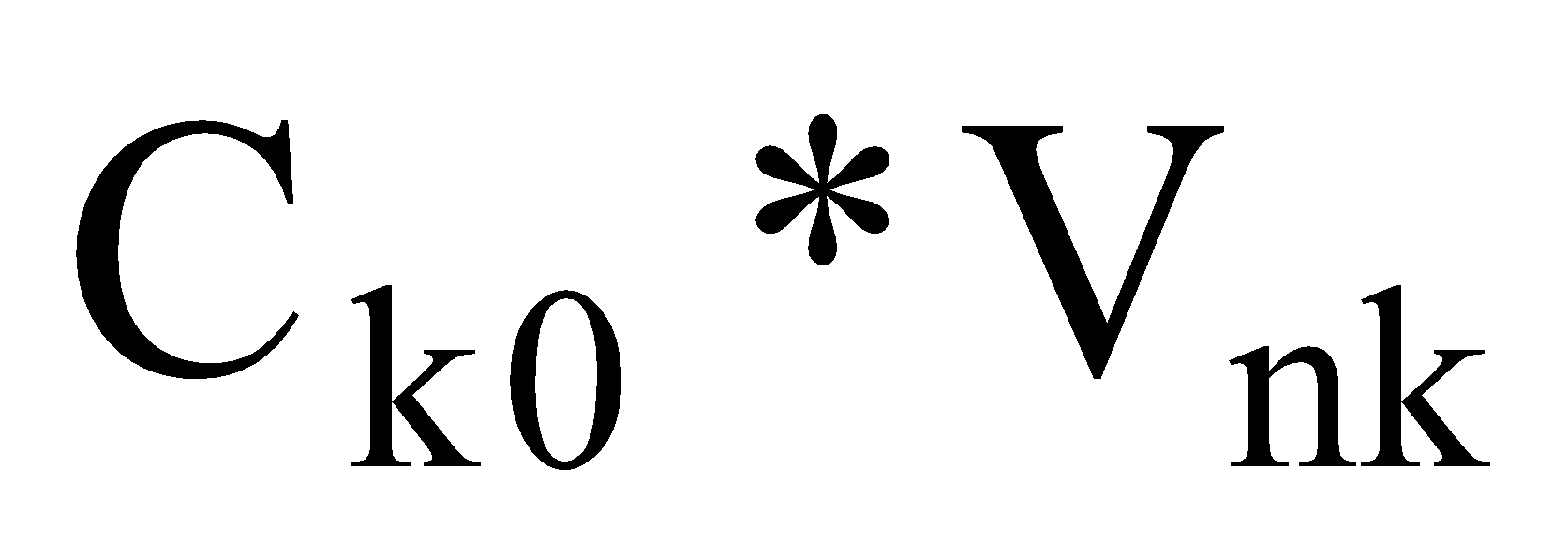
**Кратко рассмотрим методику:**

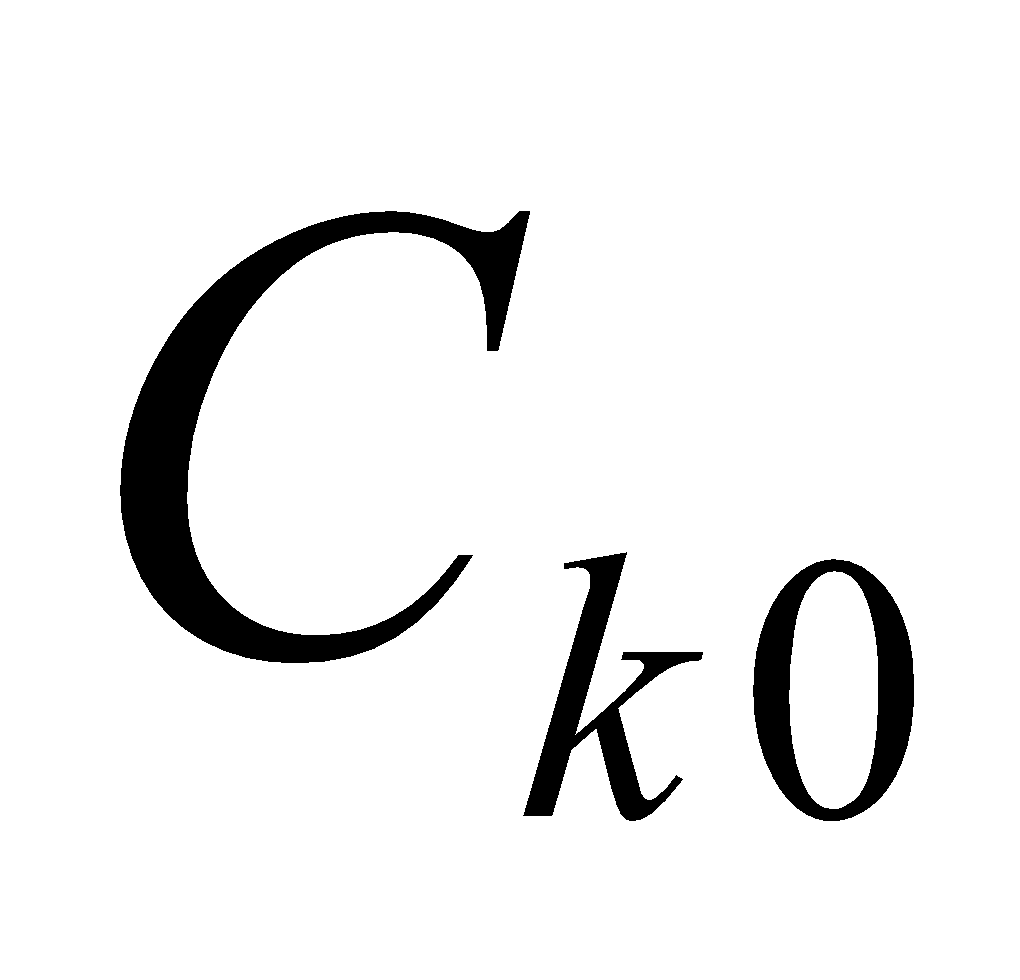
1. Проводится декомпозиция ОИ на составляющие подсистемы – сегменты.
2. Определяется объем и рассчитывается стоимость защищаемой информации в n-ом сегменте по формуле:

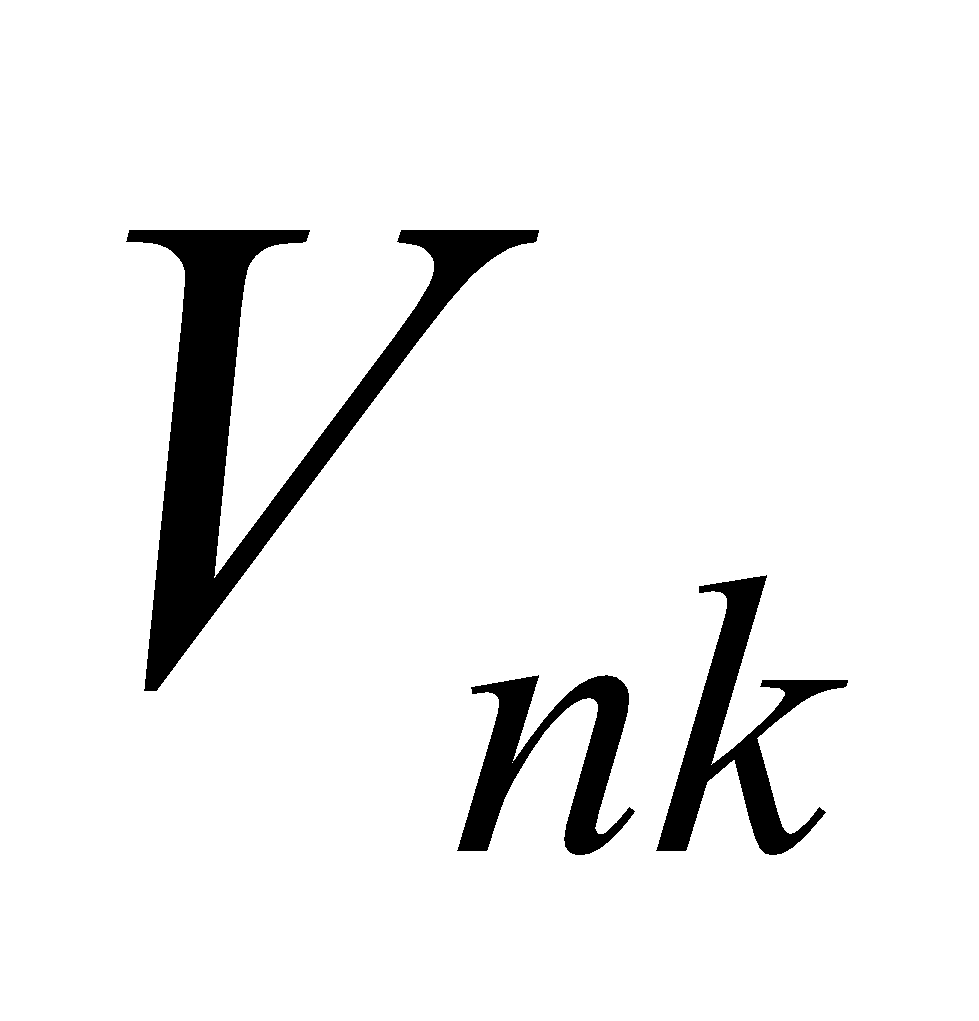
*Cn=Cn1+.. +…CnK=* (1),

где K – число уровней ограничения доступа (категорий важности) информации, циркулирующей в n-ом сегменте.

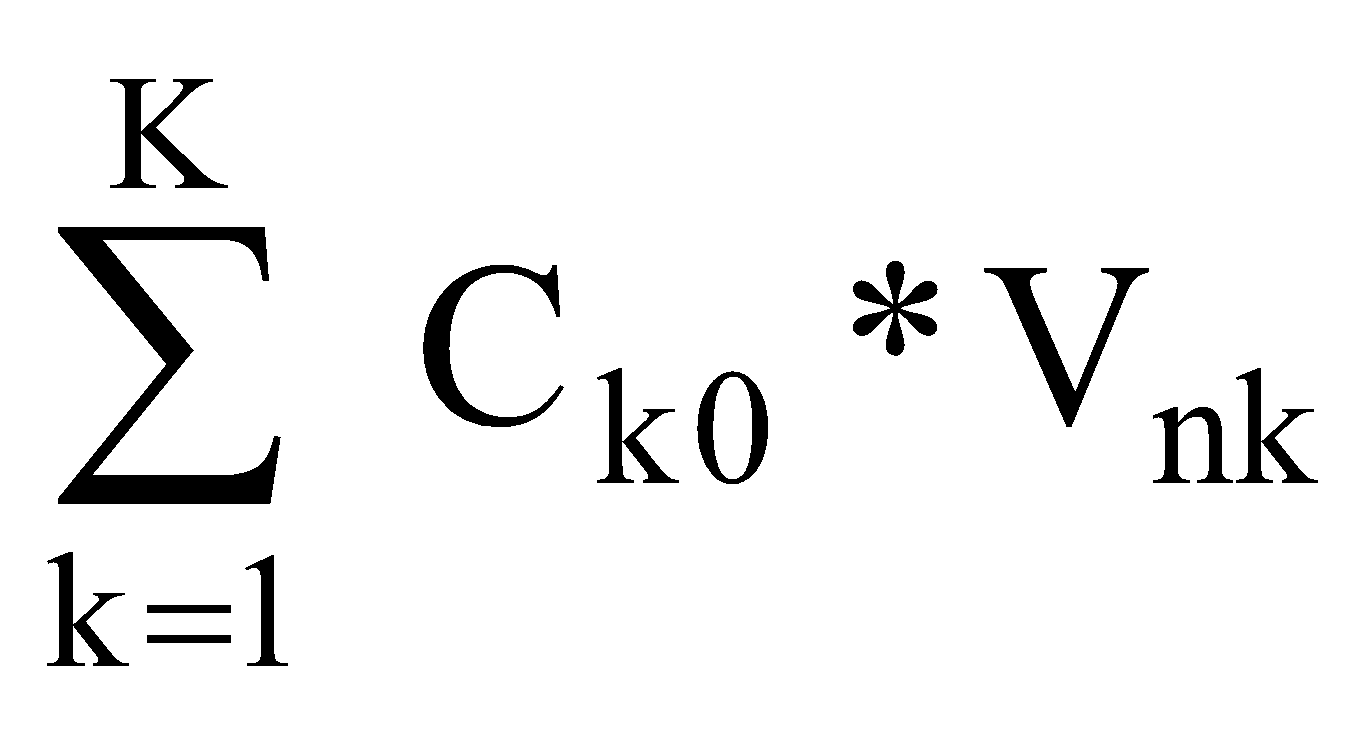
Стоимость информации k-ой категории важности в n-ом сегменте рассчитывается по формуле [5]:

*Cnk=* (2),

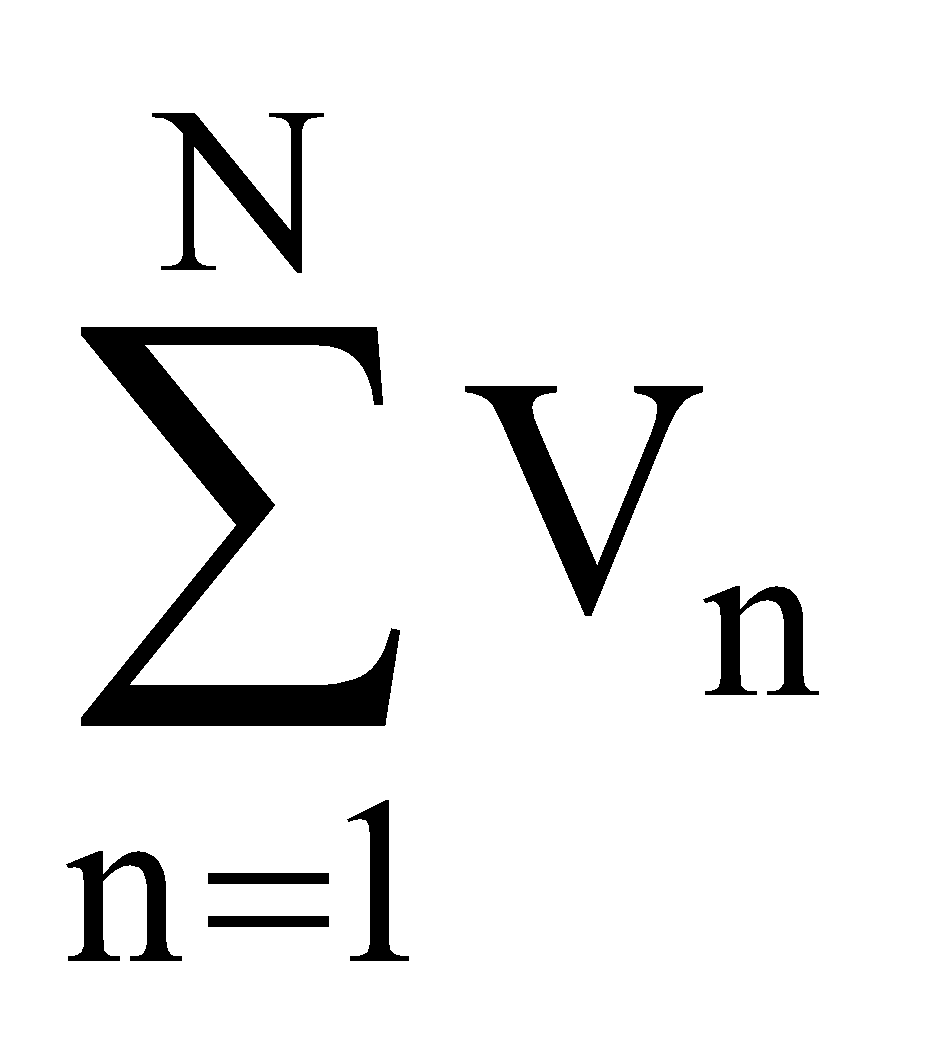
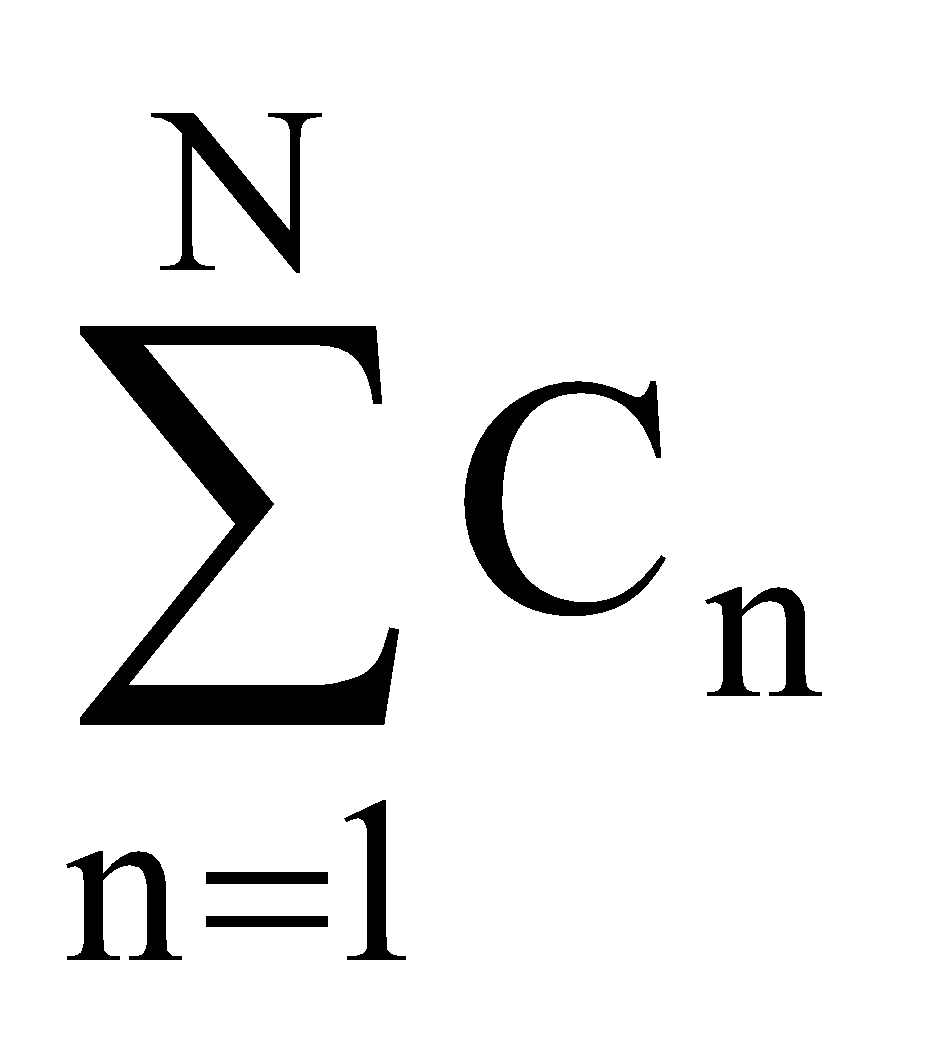
где - - стоимость единицы объема информации k-категории важности,

-объем информации k-категории важности в n сегменте.

Тогда формула (1) с учетом (2) приобретает вид

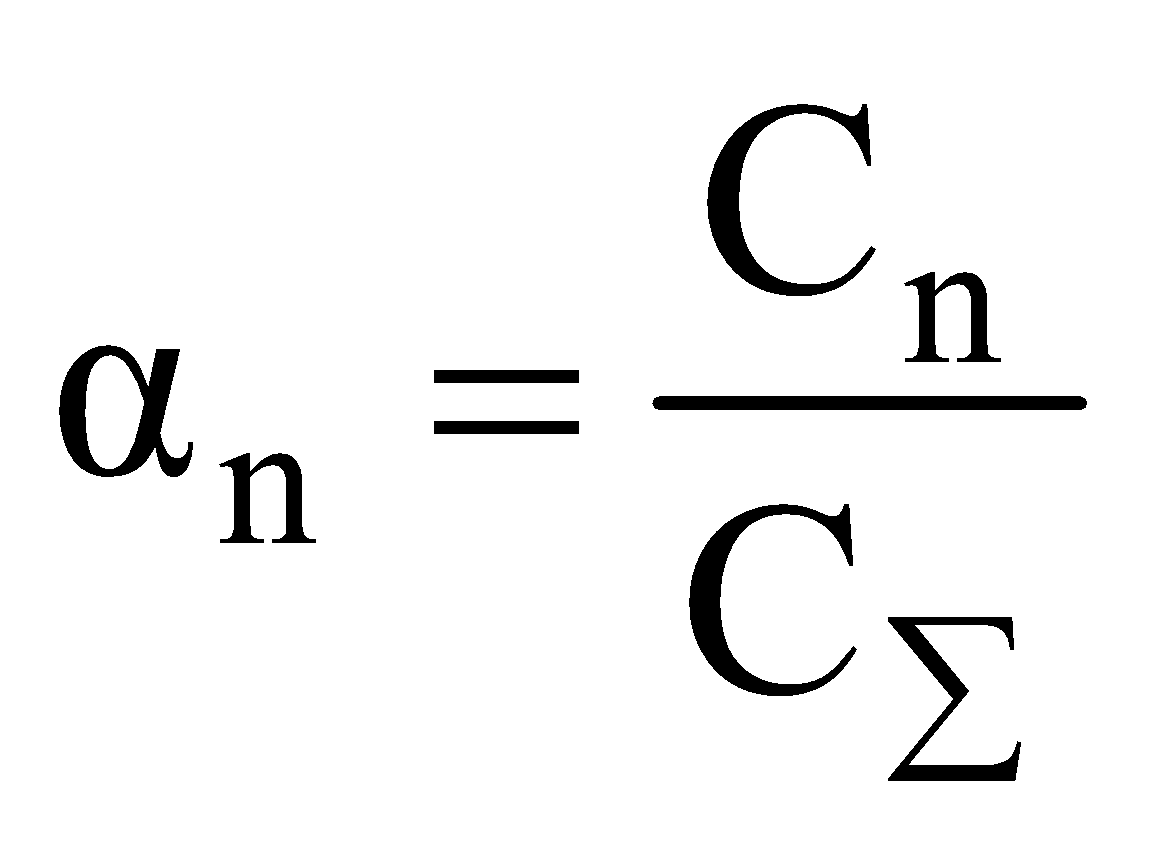
*Cn=* (3).

3. Определяется объем (V∑)и цена (C∑) информации, подлежащей защите, циркулирующей на ОИ:

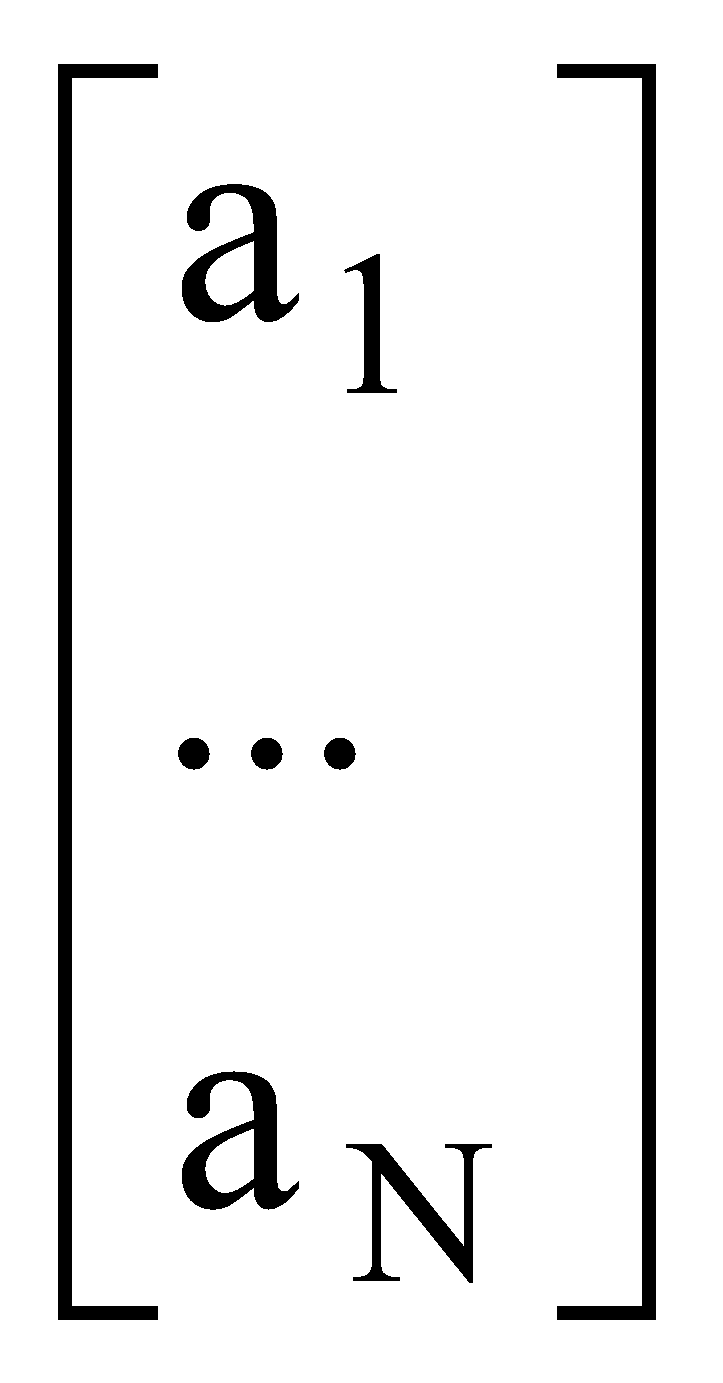
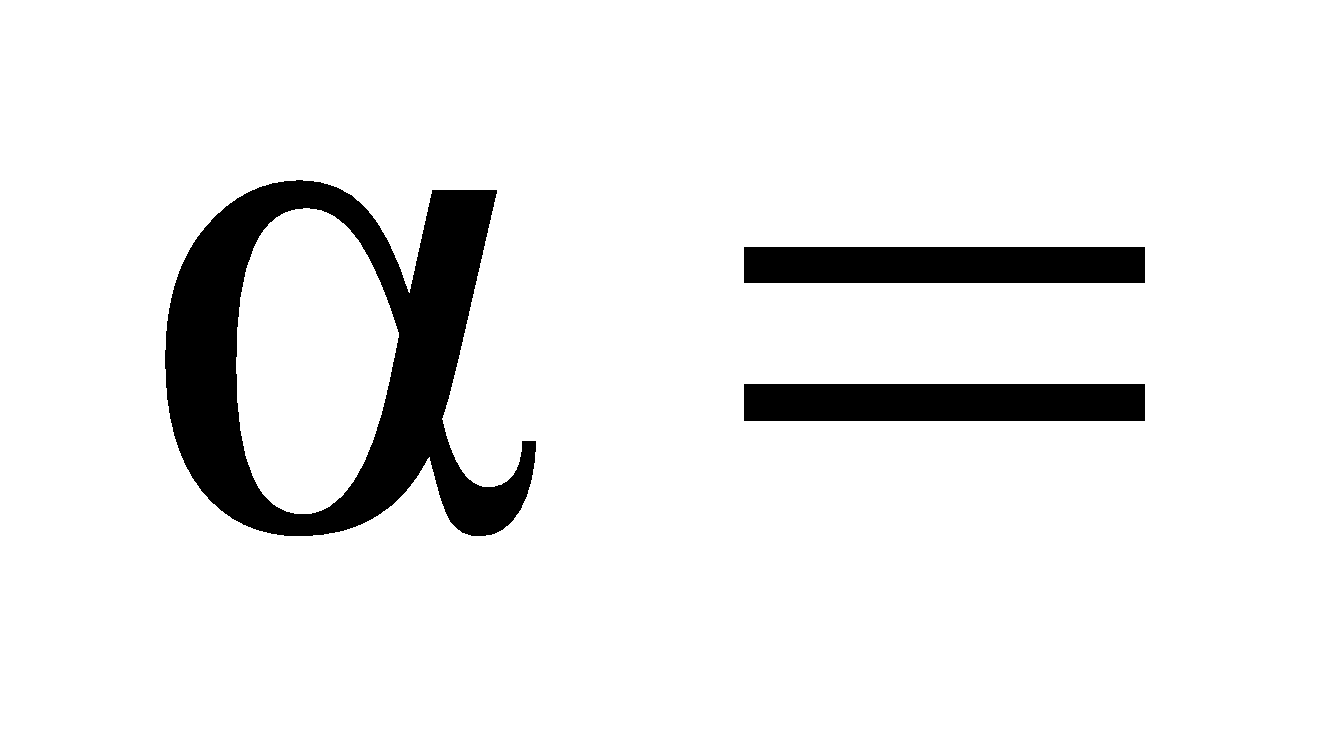
*V∑ =*(4), *C∑ =* (5),

где N – число сегментов на ОИ.

4. Определяются коэффициенты ущерба по формуле

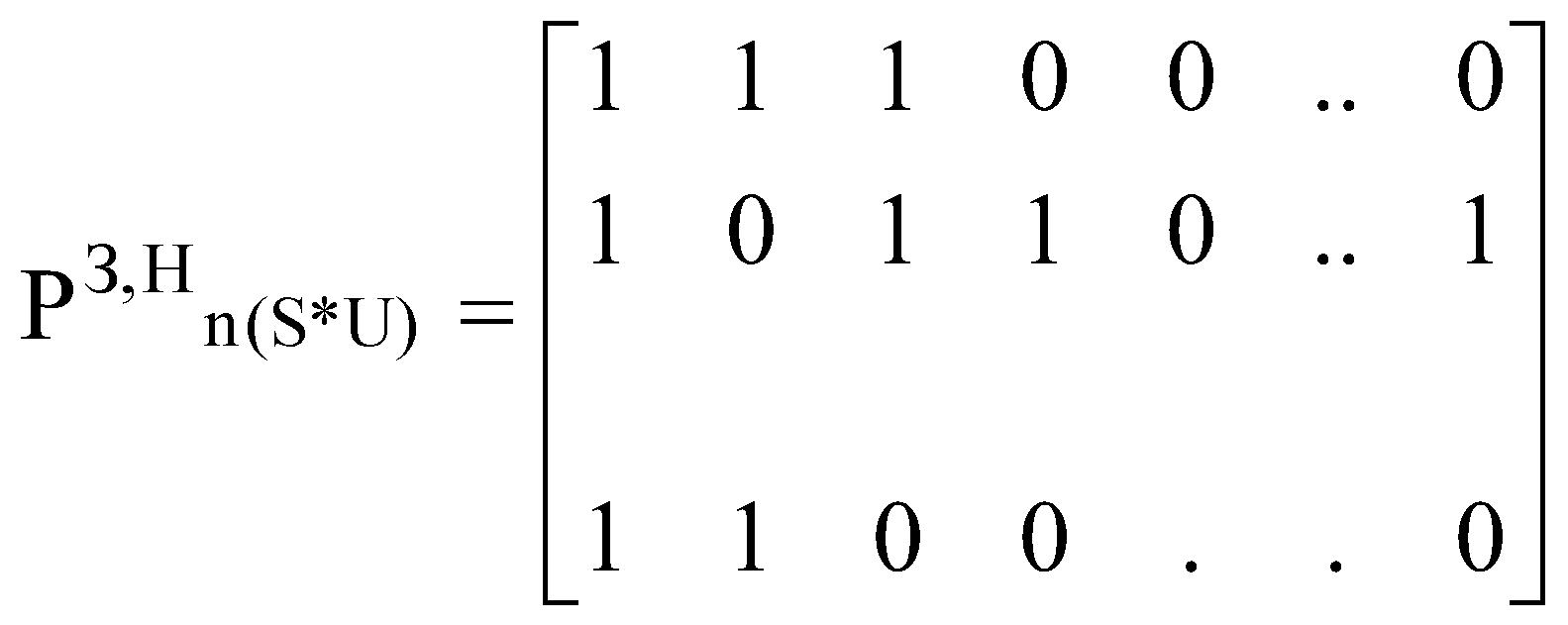
 (6),

где αn - доля ущерба, который может быть нанесен в случае реализации угроз информации в n-ом сегменте ОИ.

;

5. Описывается множество каналов НСДУВ ОИ, которые могут привести к нарушению конфиденциальности, целостности, доступности.

Описывается множество каналов {S}, реализация которых возможна в данном сегменте. Множество каналов НСД УВ, реализация которых возможна в сегменте, может быть описано в матричном виде, например

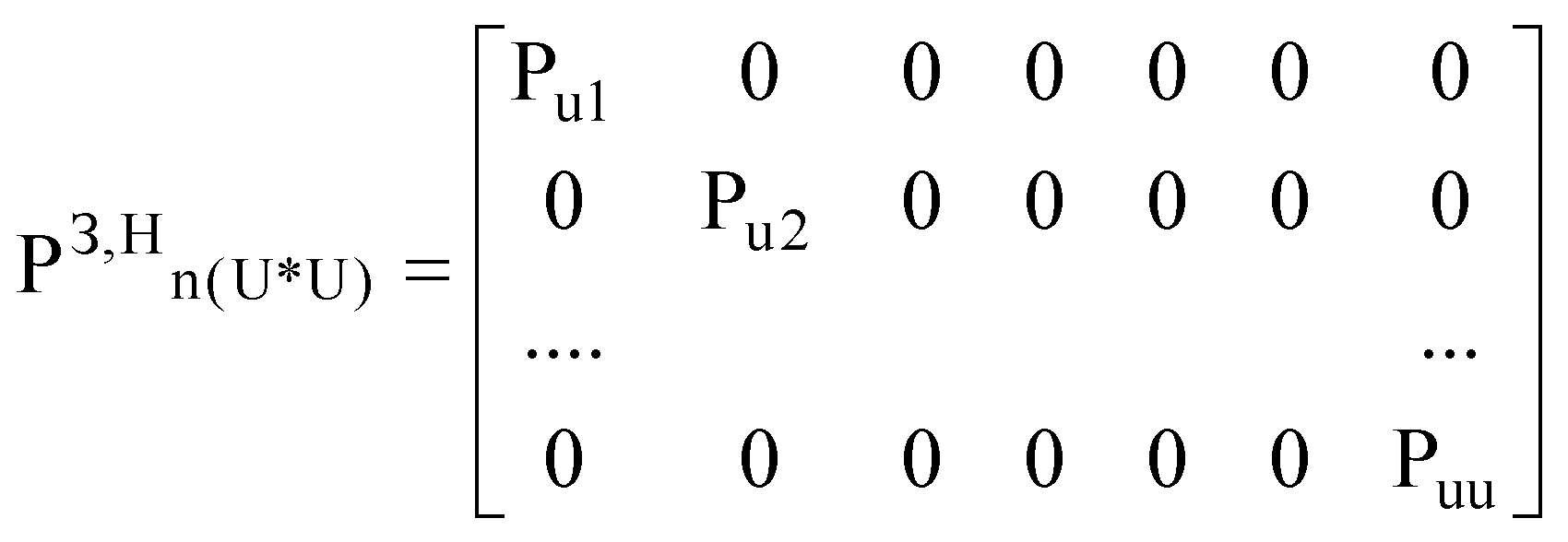
,

где число строк в матрице равно числу s потенциально возможных в n-ом сегменте каналов НСД УВ, sЄS, число столбцов равно максимальному числу элементов угроз.

Таких матриц формируется две для каждого сегмента. Одна отображает потенциально возможные действия злоумышленника, а другая – нарушителя.

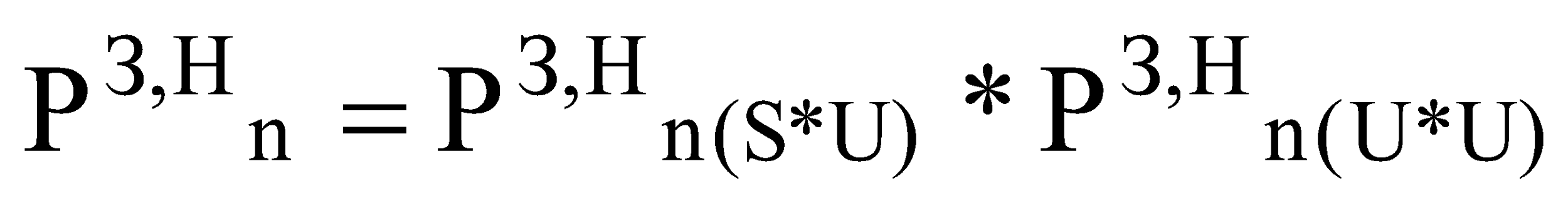
В строке единицы указывают задействованные в канале элементы угроз.

6. Далее для каждого сегмента составляется две диагональные квадратные матрицы. В одной матрице по диагонали вписаны вероятности элементов угроз для случая реализации угрозы злоумышленником, в другой – нарушителем. Пример такой матрицы для n-го сегмента

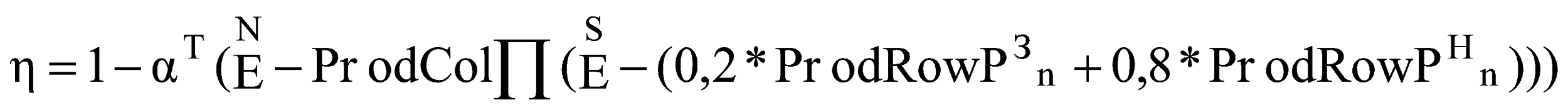
,

Puu – вероятность реализации элемента угрозы. Число строк и столбцов в этой матрице равно U.

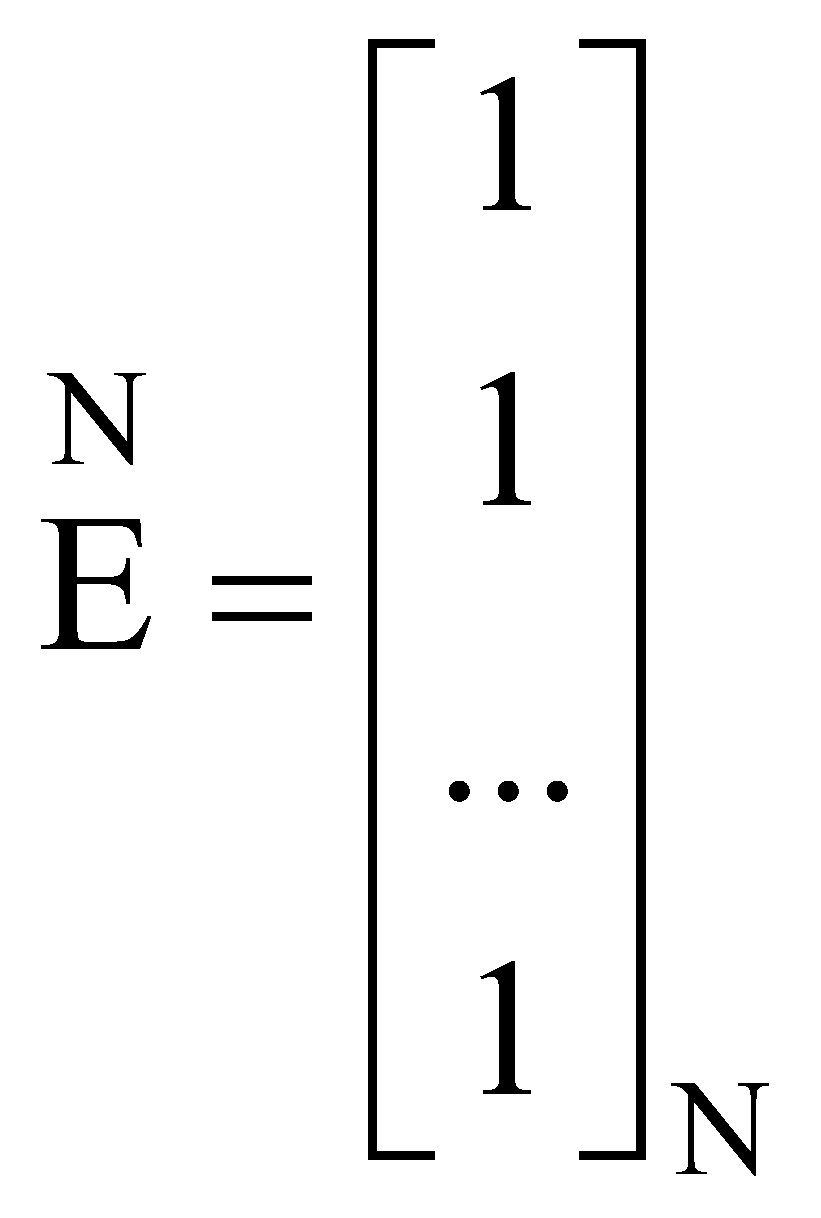
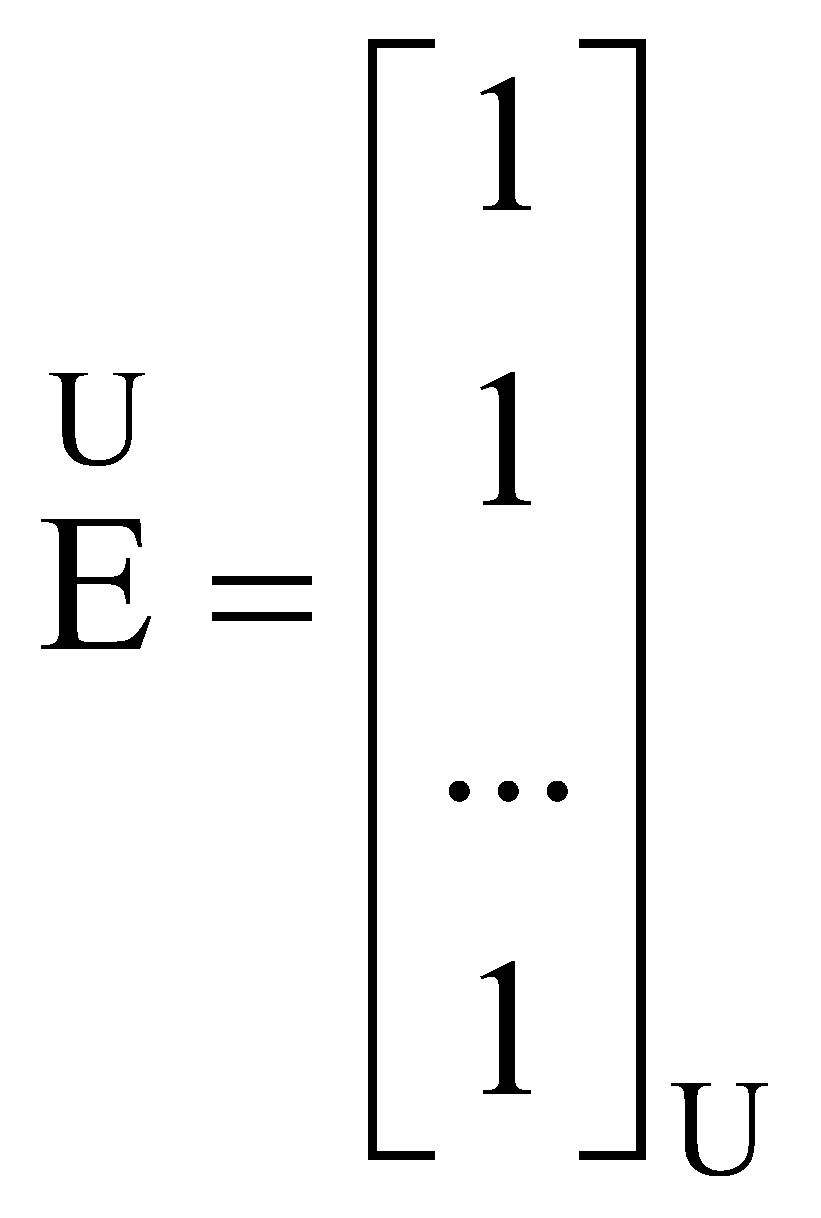
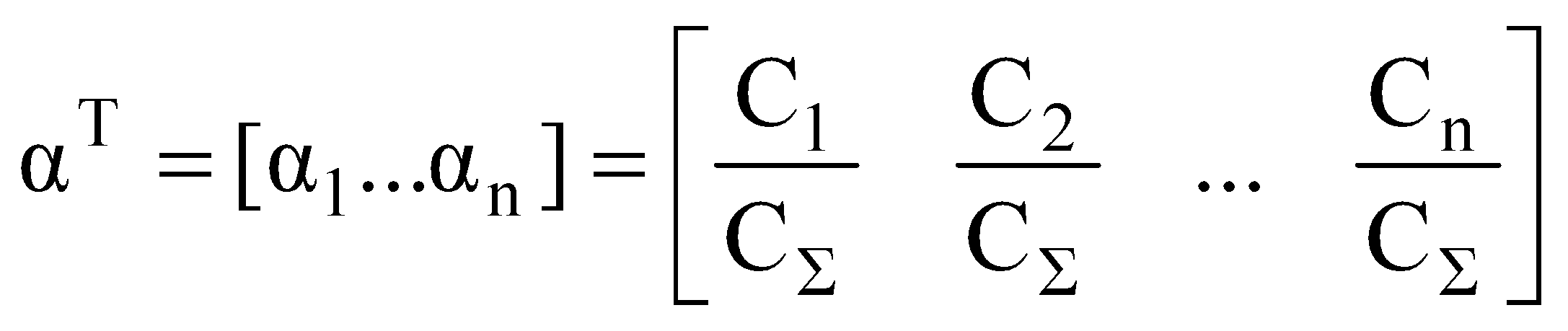
7. Вычисляется матрица угроз нарушителя и матрица угроз злоумышленника.



1. После этого степень защищенности может быть вычислена по формуле

,

где ProdRow – операция умножения ненулевых элементов в строке матрицы; ProdCol – операция умножения ненулевых элементов столбцов;

;;.

Используя предложенный подход, можно сравнивать различные комплексы средств защиты по уровню защищенности, обеспечивая требуемый уровень защиты с учетом экономичности безопасности.

Таким образом, основное назначение разработанной модели угроз состоит в создании предпосылок для объективной оценки общего состояния информационной системы с точки зрения уровня защищенности информации в ней.

Основной направленностью этой модели является не просто оценка угроз информации как таковых, а еще и оценка потерь, которые могут иметь место при реализации различных угроз. Необходимость в таких оценках возникает при анализе ситуации защищенности ОИ с целью выработки решений по организации защиты информации.

**Библиографический список**

1. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. –СПб.: Наука и техника, 2004.–384 с.

2. Варламов О. О. Системный подход к созданию модели компьютерных угроз информационной безопасности.// Материалы VI Международной научно-практической конференции «Информационная безопасность»- Таганрог: Издательство ТРТУ, 2004 С. 61-65 .

3. Домарев В. В. Безопасность информационных технологий. Системный подход: - К.: ООО ТИД ДС, 2004.-992с.

4. И. В. Машкина, Е. А. Рахимов. Модель объекта информатизации // Материалы VI Международной научно-практической конференции «Информационная безопасность»- Таганрог: Издательство ТРТУ, 2004. С.

5. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам//Гротек, 1997, 248 с.