Компания Ай Ти; ДМК Пресе, 2004. - 348с. ***8.*** *Андрощук Г. А., Крайнєє П.П. Зкономическая безопасность предприятия: защита коммерческой тайньї. - К: Изд. Дом «Ин Юре», 2000. – 400 с.* ***9.*** *Гринберг А. С., Горбачев Н. Н., Тетяков А. А. Защита информационньїх ресурсов государственного управлений. - М.: Юнити-ДАНА, 2003. – 327 с.* ***10.*** *Фатьянов А. А. Проблеми защитьг конфиденциальной информации, не составляющих государственную тайну//Информационное общество. - № 1. – 1997. - с. 49 - 56.* ***11.*** *Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності. Затверджено Держкомсекретів України, наказ №2 3 від 9. 02. 1998 р.* ***12.*** *Гостев И.М. Безопасность - бесполезная трата денег или их выгодное вложение?// Конфидент. Защита информации. - № 5. - 2003. - с. 16 - 18.*

УДК 65.012.8:330.131.5

МЕТОДИКА ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Светлана Гришко, Сергей Резников

Харьковский национальный университет радиоэлектроники

Аннотация: **Предлагается методика оценки экономической эффективности для комплексной системы защиты информации. Она позволяет определить ценность информации, находящейся в данной организации, оценить возможный ущерб от различных действий злоумышленника, сравнить разные варианты защиты и выбрать оптимальное соотношение по принципу «цена-качество».**

Summary: **The method of estimation of economic efficiency for the complex system of defence of information is offered. It allows to define the value of information being in this organization; to estimate possible harm from different actions of malefactor; to compare different variants of defence and choose optimum correlation on the principle «price-quality».**

Ключевые слова: **Эффективноссть защиты информации, стоимость защиты информации, информмационная ценность.**

Введение

Для функционирования любой структуры, будь то государственная, предпринимательская или общественная организация, необходимы разнообразные ресурсы: материальные, трудовые, финансовые. Но в современных условиях все большее значение приобретает еще один вид ресурсов – информационный. Специфика информации, как и любого другого нематериального актива, состоит в том, что она не имеет материальной формы и, как правило, жесткой привязки к носителю, а ее хищение может быть произведено путем простого копирования, т. е. без физического изъятия объекта.

Такие особые свойства, а также ценность информационного ресурса заставляет уделять все больше внимания вопросам защиты информации. Для их решения требуются значительные финансовые средства.

Поэтому в сфере обеспечения безопасности информации возникает классическая **проблема экономической эффективности –** поиск оптимального соотношения затрат и результатов. Здесь это означает, что нужно найти наилучшее сочетание организационно-технических решений по защите информации с затратами на их осуществление.

Вопросы экономической эффективности давно и детально исследовались как отечественными, таки и зарубежными специалистами. Можно выделить такие основные направления экономического обоснования:

- обоснование экономической эффективности некоммерческих инновационных проектов, которое проводится на основе сопоставления капитальных и эксплуатационных затрат, определения срока окупаемости; такая методика, в частности, рассматривается в [1, 2];

- обоснование экономической эффективности инвестиционных проектов, которое проводится на основе таких показателей: чистый приведенный доход, индекс доходности, индекс рентабельности; на наш взгляд, этот подход лучше всего рассмотрен в [3], кроме того, существует и нормативный документ для такого обоснования – методика [4].

Эти хорошо известные подходы не могут быть применены к оценке эффективности системы защиты информации. Они рассматривают в качестве результата от внедрения предлагаемых решений **изменение качества объекта** - например, улучшение технических характеристик, прирост дохода, экономию ресурсов. В нашем случае результатом будет **сохранение качества объекта**, отсутствие (или уменьшение)

последствий, которые возможны при утечке информации. Такой результат сложно подсчитать в натуральных единицах измерения, он скорее представляет собой снижение рисков функционирования системы.

Похожие проблемы решают, например, при оценке систем пожарной безопасности [5]. Но и этот подход здесь не применим. Во-первых, он основан на определении математического ожидания, поэтому предполагает наличие статистики происшествий и их последствий. Этой статистики для информационных систем, как правило, нет и быть не может из-за "уникальности" последствий для каждой системы. Во-вторых, он основан на оценке прямого материального ущерба, чего не происходит при утечке информации. В последнем случае ущерб можно определить лишь косвенно, хотя его размеры могут существенно превышать материальные потери от пожара.

Цель данной статьи – предложить методику, которая позволила бы оценить экономическую эффективность системы защиты информации.

I Общие методические основы

Под **комплексной системой защиты информации (КСЗИ)** будем понимать совокупность организационных и инженерных мер, программно-аппаратных средств, обеспечивающих защиту информации, т. е. предотвращение нарушения ее конфиденциальности, целостности и доступности [6].

Оценку такой системы предлагается осуществлять на основе классического принципа экономической эффективности - сопоставления объема затрат на обеспечение безопасности информации, с одной стороны, и эффекта, получаемого от функционирования КСЗИ, с другой.

В качестве эффекта функционирования КСЗИ предлагается рассматривать сохранность ценности информации, которая есть у данной структуры, за определенный период времени.

Расчетный период – это время, на которое определяются затраты и результаты функционирования КСЗИ. Далее примем за расчетный период год.

Методика расчета экономической эффективности КСЗИ включает 4 этапа:

1 этап – определение информационной ценности для данной структуры на расчетный период времени;

2 этап – определение возможных убытков от нарушения конфиденциальности, целостности и доступности информации;

3 этап – определение затрат на организацию КСЗИ и ее эксплуатацию;

4 этап – расчет показателя экономической эффективности, который отражает, сколько информационной ценности сохраняет каждая гривна расходов на КСЗИ.

II Определение ценности информации данной структуры

Ценность объекта в широком смысле рассматривается как его значимость для человека, социальной группы, общества в целом.

Ценность как экономическая категория – это полезность, то есть способность продукта удовлетворять те или иные потребности. Она определяется суммой благ, которые данный продукт предоставляет пользователю.

Уже много лет в экономике существует направление, изучающее вопросы ценности, - это концепция субъективизма. В начале 20-го века его представляла австрийская школа (Э. Бем-Баверк, К. Менгер и др.). Занимались этими вопросами и известные украинские экономисты (М. Туган-Барановский, Р. Оржентский). Позже на этой основе сформировалась школа маржинализма, которая и сегодня не утратила своей актуальности. Многие фундаментальные экономические теории связаны с исследованием ценности. К этим проблемам обращались такие экономисты, как К. Маркс [7], И. Фишер [8], лауреаты Нобелевской премии Дж. Хикс [9], М. Фридмэн [10], П. Самуэльсон [11] и другие.

Но при разных взглядах на суть и роль ценности, авторы сходны в одном: ценность – категория субъективная, ее величина зависит от восприятия продукта человеком.

Расчет ценности информации – это сложная научно-методическая проблема. Она усложняется тем, что информация – это специфический продукт, и ее важность можно рассматривать только в контексте данной организации, окружающей ее среды и на данный момент времени. Это означает, что в основе количественного расчета ценности информации должен находиться экспертный опрос ее пользователей.

Еще более актуальной прикладной задачей является стоимостная оценка ценности информации. Ее решение заключается в переводе информационной ценности в денежные единицы. Сложность же состоит в том, что необходимо найти критерий, по которому субъективный параметр (ценность) получит объективную оценку. Эта задача заслуживает отдельного и более подробного изучения.

Проблему, которую рассматриваем в рамках данной статьи – обоснование выбора КСЗИ, лучше решать

без стоимостной оценки ценности информации. Для сравнения разных КСЗИ важны не абсолютные значения, а относительные: насколько больше или меньше информации защитит данная КСЗИ по сравнению с другими системами.

Поэтому предлагается рассчитать балльную оценку ценности информации на основе экспертного опроса.

Данный этап предполагает работу со специалистами заказчика, которые знают свою информационную систему, информационные потоки и виды, в которых информация существует в организации. Данные, необходимые для расчетов на этом этапе, можно получить путем экспертного опроса таких специалистов и оформить, например – для коммерческих структур, в виде раздела Положения о коммерческой тайне.

Прежде всего, заказчику необходимо определить, какая информация представляет ценность для организации и подлежит защите.

Назовем такую информацию **конфиденциальной** и будем понимать под этим сведения, находящиеся во владении, пользовании и распоряжении отдельных лиц и распространяющиеся по их желанию в соответствии с предусмотренными ими условиями.

Затем следует всю такую информацию классифицировать по видам, в которых она существует. Например:

- информация в письменном виде (сюда можно отнести и печатные, и рукописные документы);
- информация в электронном виде (в ПК, на CD и т. п.);
- видеоинформация (например, собираемая с видеокамер);
- звуковая информация (которая, например, передается во время личных или телефонных разговоров на контролируемой территории).

После этого по каждому виду информации определяется ее объем, измеряемый в Мб. Например, печатный текст может измеряться по соотношению 1 символ – 1 байт, 1 акустическая минута – 10 Мб.

Обозначим каждый вид информации через n, а соответствующий ей объем через Q_n и занесем полученный данные в таблицу "Объем информационных ресурсов". Пример такой формы представлен в табл. 1.

Таблица 1 – Объем информационных ресурсов

Вид информации	Объем (Мб)
1. Информация в письменном виде	
1.1 Учредительные документы	0,9 Мб
1.2 Отчетность за t-ый период и т. д.	0,3 Мб
…	…
n-й вид информации	Qn

Но большой объем информации может представлять гораздо меньшую ценность, чем информация малого объема. Поэтому объем информационного ресурса необходимо скорректировать на его ценность.

Для этого каждый вид информации нужно разбить на группы по степени ее важности для данной структуры. Эти данные также можно получить с помощью экспертного опроса специалистов заказчика. Пример подобной классификации приведен на рис.1. В зависимости от организационной структуры и отребностей заказчика классификация может быть более детализированной.

Затем каждой группе присваивается балльная оценка важности такой информации (например, по 100-балльной шкале) и определяется время, в течение которого информация сохраняет указанную важность (например, в днях)

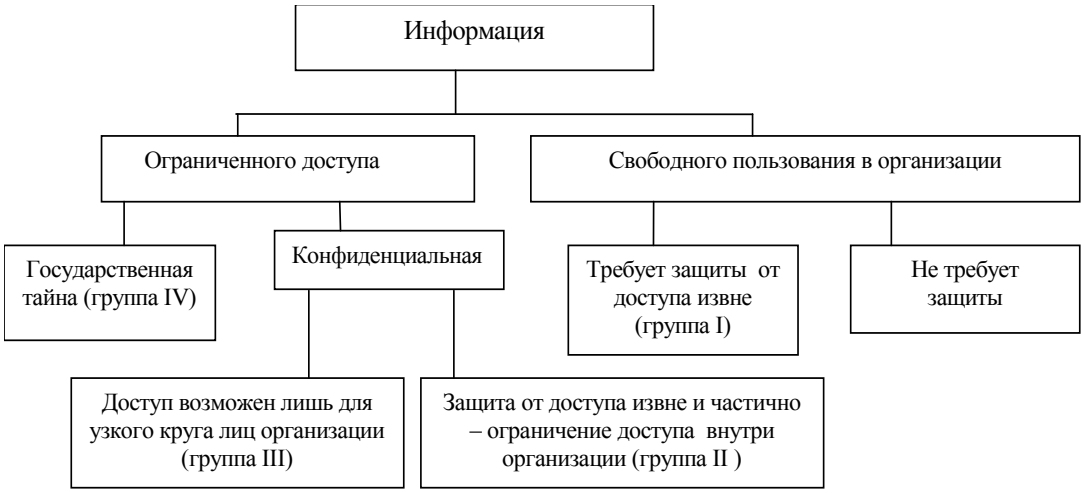

Рисунок 1 – Пример классификации информации по степени важности

Теперь для каждого n-го вида информации можно подсчитать информационную ценность единицы по формуле (1).

$$In = Б \cdot \frac{Tn}{365\ дней} \qquad (1)$$

где In – информационная ценность единицы n-го вида информации, Б – балльная оценка важности информации, баллы, Tn - время, в течение которого информация сохраняет указанную важность, дни, 365 дней – число дней в расчетном периоде.

На основе полученных данных определим информационную ценность каждого n-го вида информации wn по формуле:

$$Wn = Qn \times In. \qquad (2)$$

Эти данные и будут основой для вычисления результата функционирования КСЗИ. Их также следует занести в таблицу (см. табл. 2).

Таблица 2 – Определение ценности информационных ресурсов системы

Вид информации	Объем Qn, Мб	Ценность единицы информации (Б), баллы	Время, за которое сохраняется важность (Tn), дни	Ценность информации (wn), Мб-баллы
1.1 Учредительные документы	0,9 Мб	80	365	72
1.2 Отчетность за t-ый период и т. д.	0,3 Мб	40	180	5,9
…	…	…	…	…
n-й вид информации	Qn	In	Tn	wn
Итого информационная ценность всей структуры	$W = \sum Wn$			

На основе полученной информации можно рассчитать и информационную ценность всей структуры (обозначим ее как W).

Таким образом, информационная ценность всей структуры W определяется как суммарный объем информации, скорректированный на ее важность.

III Определение возможных убытков от утечки информации

Для того, чтобы сохранить информационную ценность структуры W в течение расчетного периода, необходимо принять меры безопасности. Если этого не сделать, может произойти утечка информации, ее блокировка или нарушение целостности, что приведет к полной или частичной потере информационной ценности структуры.

Поэтому цель системы защиты информации – полное или частичное сохранение информационной ценности W в течение расчетного периода.

При внедрении КСЗИ заказчик сохранит определенную величину информации. Обозначим ее как $W_{ксзи}$. Этот объем будет меньше всей информационной ценности W, т. к. защита происходит с определенной

вероятностью и остается возможность того, что мероприятия по защите информации не достигнут своей цели.

Но без внедрения КСЗИ заказчик потеряет всю информацию n-го вида. Хотя в любом случае даже без внедрения КСЗИ при самых мощных действиях злоумышленников какая-то часть информации останется. Обозначим ее W «без КСЗИ»

Результатом работы КСЗИ (это и есть экономический эффект) можно рассматривать разницу между ценностью информации, которую заказчик сохранит при внедрении КСЗИ, и ценностью информации, оставшейся у заказчика после действий злоумышленников без внедрения КСЗИ:

$$эффект = W\ ксзи - W"без\ ксзи" \quad (3)$$

Таким образом, на данном этапе предстоит определить возможные действия злоумышленников и оценить их результаты.

Вначале нужно выяснить, по каким каналам возможна утечка информации каждого n-го вида. На основе таких данных можно предположить возможные действия злоумышленника (обозначим их как Ai).

Чтобы противодействовать злоумышленнику, в КСЗИ могут использоваться различные способы защиты (обозначим их как Bj). В качестве Bj можно принимать и отдельную аппаратуру, но рекомендуется рассматривать варианты организации КСЗИ в целом.

Каждый из этих способов может быть реализован с помощью аппаратуры разного качества. Поэтому один и тот же способ Bj позволит осуществлять защиту информации с разной вероятностью. Обозначим j-тую вероятность защиты информации j-тым способом как Pjk.

Теперь можно рассчитать, какая информация будет сохранена при использовании Bj способа защиты, и какая информация останется, если этого не сделать.

Величина представляет собой разницу между всей информационной ценностью W и той информацией, которая может быть потеряна даже при внедрении Bj способа защиты:

$$W_{ксзи} = W - \sum W_n \times (1 - P_{jk}). \quad (4)$$

Величину W «без ксзи» можно определить как разницу между ценностью всей информации W и информацией n-го вида, утерянной в результате действий злоумышленника:

$$W_{"без\ ксзи"} = W - \sum W_n. \quad (5)$$

Таким образом, эффект от защиты Bj способом равен:

$$эффект = W\ ксзи - W"без\ ксзи" = \sum Wn \times P_{jk} \quad (6)$$

Все возможные варианты результатов Bj способов защиты при Ai действиях злоумышленника можно представить в виде матрицы:

Таблица 3 – Информация, сохраненная при использовании Bj способа защиты и Ai действиях злоумышленника

Действия злоумышленника	Защита B_1 с вероятностью			…	Защита Bj с вероятностью		
	P_{11}	P_{12}	P_{13}	…	P_{j1}	P_{j2}	P_{jk}
A_1	$W_1 \cdot P_{11}$	$W_1 \cdot P_{12}$	$W_1 \cdot P_{13}$	…	$W_1 \cdot P_{j1}$	$W_1 \cdot P_{j2}$	$W_1 \cdot P_{jk}$
A_2	$W_2 \cdot P_{11}$	$W_2 \cdot P_{12}$	$W_2 \cdot P_{13}$	…	$W_2 \cdot P_{j1}$	$W_2 \cdot P_{j2}$	$W_2 \cdot P_{jk}$
…							
Ai	$Wi \cdot P_{11}$	$Wi \cdot P_{12}$	$Wi \cdot P_{13}$	…	$Wi \cdot P_{j1}$	$Wi \cdot P_{j2}$	$Wi \cdot P_{jk}$

IV Определение затрат на организацию КСЗИ и ее эксплуатацию

Каждый из рассматриваемых способов защиты информации предполагает приобретение и эксплуатацию технических средств. Это означает, что у заказчика возникнут определенные затраты, которые будут разниться в зависимости от избранного варианта защиты Bj.

Для оценки экономической эффективности и выбора варианта КСЗИ следует рассчитать затраты по каждому из предлагаемых вариантов защиты информации Bj.

Выделяют два вида затрат, необходимых для осуществления подобных технических проектов: инвестиционные и эксплуатационные.

Инвестиционные затраты – это единоразовые вложения капитала в разработку и организацию КСЗИ. К таким затратам можно отнести расходы на:

- создание проекта КСЗИ (куда, в том числе, можно отнести и затраты на оценку экономической эффективности разных КСЗИ);
- покупку необходимых основных фондов: техники и оборудования, программного обеспечения, средств связи и т. п.;

- организацию линий связи;
- инсталляцию КСЗИ и приспособление ее к условиям данной структуры;
- обучение персонала.

Это не окончательный перечень, он может быть дополнен или сокращен в зависимости от предлагаемых вариантов КСЗИ. Просуммировав все эти затраты, получаем общую сумму необходимых инвестиций в данный проект.

Но следует учитывать, что КСЗИ, внедренная в результате такого инвестирования, может использоваться (амортизироваться) гораздо дольше, чем расчетный период. Следовательно, на расчетный период нужно отнести лишь часть инвестиционных затрат. Расчет этой части зависит от способа амортизации, принятого заказчиком.

Например, при прямолинейном способе обеспечивается равномерная амортизация объекта в течение срока его использования. При этом годовая сумма амортизации определяется делением амортизируемой стоимости на ожидаемый период времени использования объекта:

$$ИЗ_{год} = \frac{инвестиционные\ затраты}{срок\ использования\ (в\ годах)}. \qquad (7)$$

Таким образом, показатели разных инвестиционных затрат становятся сопоставимыми по времени.

К эксплуатационным относят затраты, которые необходимы для нормального функционирования предлагаемой КСЗИ в течение расчетного периода. Структура эксплуатационных затрат также может изменяться в зависимости от предлагаемых решений.

В общем случае эксплуатация КСЗИ может потребовать от заказчика таких текущих расходов:

- зарплата специалистов, занятых в работе КСЗИ, с начислениями;
- оплата услуг связи;
- оплата электроэнергии;
- расход сырья, материалов, комплектующих и МБП;
- оплата работ (услуг) сторонних организаций (например, для получения информации) и другое.

Итого, общие затраты по варианту Bj на расчетный период определяем по формуле:

$$З_j = ИЗ_{год} + ЭЗ_{год}, \qquad (8)$$

где $З_j$ - затраты на организацию и эксплуатацию СЗИ по варианту Bj на расчетный период (год); $ИЗ_{год}$ – инвестиционные затраты, амортизируемые за расчетный период, определяются по формуле (7); $ЭЗ_{год}$ – эксплуатационные затраты за расчетный период.

V Оценка экономической эффективности

С экономической точки зрения эффективность любого проекта (в том числе и проекта по защите информации) определяется как соотношение эффекта от внедрения предложенных идей и затрат на их реализацию. Для каждого j-го варианта КСЗИ нужно рассчитать такой показатель эффективности:

$$эффективность = \frac{эффект}{затраты} = \frac{\sum W_n \times P_{jk}}{З_j}. \qquad (9)$$

Он показывает, какую информационную ценность удастся сохранить в расчете на одну гривню расходов. Чем выше этот показатель, тем более эффективной считается КСЗИ.

Но выбор КСЗИ можно осуществлять не только по критерию максимизации показателя эффективности. Ведь у заказчика могут быть свои представления о том, какую КСЗИ считать оптимальной.

Данные, полученные в результате ранее проведенных расчетов, позволяют использовать стандартные методы исследования операций. Например, заказчик может выбрать один из следующих критериев:

- критерий оптимиста (max max) означает, что заказчику нужна максимальная эффективность при максимальных расходах на защиту информации;
- критерий пессимиста (max min), когда за минимальную сумму нужно построить максимально защищенную систему;
- критерий относительного пессимиста (min max), когда не имеет значения, сколько вкладывать средств, главное – заблокировать канал утечки информации.

Кроме того, возможно установление ограничений по стоимостным показателям, по срокам, надежности или другим факторам. После того, как критерий и ограничение избраны, составляется оптимизационная модель.

Выводы

Информация и поддерживающие ее системы и сети являются ценными ресурсами. Из-за растущей зависимости организаций от информационных систем они становятся более уязвимыми. Использование систем защиты информации позволяет в большей или меньшей степени решить эту проблему, но требует определенных финансовых средств. Предложенная методика позволяет:

1) определить ценность информации, находящейся в данной организации;

2) оценить возможный ущерб от различных действий злоумышленника;

3) сравнить разные варианты КСЗИ и выбрать оптимальное соотношение по принципу «цена-качество».

*Литература **1**. Плоткин Я. Д., Львов Д. С. Зкономическая зффективность новой техники. - Львов, 1986, - 143 с. **2**. Методичні вказівки до розрахунку соціального-економічної ефективності заходів науково-технічного прогресу./Марченко О І. - ВІГІ, 1991. 3. Бланк И. А. Инвестиционный менеджмент - К.: Эльга-Н, Ника-Центр, 2001.- 448 с. **4**. Методика визначення економічної ефективності витрат на наукові дослідження і розробки та їх впровадження у виробництво, затверджена наказом Мінекономіки та європейської інтеграції N 218/446 від 25.09.2001 **5**. ГОСТ 12.1.004-91. Пожарная безопасность **6**. НД ТЗИ 1.1–003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 7. Маркс К. Капитал / Маркс К., Энгельс Ф. Собрание сочинений в 30-ти томах, 2-е изд., Т.23.- М.: Госполитиздат, 1954. **8**. Fisher I. Mathematical Investigation in the Theory of Value and Prices. - N. Haven.: Gale Univers Press, 1977. - 126 p. **9**. Хикс Дж. Р., Аллен Р. Г. Пересмотр теории ценности // Теория потребительского поведения и спроса // Под ред. В. М. Гальперина. - СПб.: Экономическая школа, 1993. - 383с. **10**. Friedman M. Price Theory. A Provisional Text. - Addine: Publishing Company, 1967. - 285 p. **11**. Самуэльсон П. Экономика: Пер. с англ. - М.: Прогресс, 1964. - 844с.*

УДК 621.395:396.77

ОЦІНКА ВИТРАТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ЦИФРОВИХ СИСТЕМ КОМУТАЦІЇ

Тетяна Тардаскіна

Одеська Національна академія зв'язку ім. А. С. Попова

Анотація: **Орієнтовна оцінка витрат на систему інформаційної безпеки типової цифрової системи комутації проводиться на етапі її технічного проектування.**

Summary: **Aproximate assessment costs of information security system of the standard digital switched systems is held on the stage of technical projection**

Ключові слова: **Інформація, інформаційна безпека, оцінка витрат, функціональні послуги зв'язку.**

Вступ

Законом України «Про телекомунікації» визначені ключові завдання забезпечення інформаційної безпеки телекомунікаційних мереж: охорона таємниці телефонних розмов, телеграфної, іншої кореспонденції, захист інформації з обмеженим доступом, що є власністю держави; захист державних інформаційних ресурсів, захист інформації про споживача; захист інформації, що передається телекомунікаційними мережами; забезпечення сталості, надійності, інформаційної безпеки телекомунікаційних мереж, підтримки рівня якості та безпеки телекомунікаційних послуг [1].

Система інформаційної безпеки телекомунікаційних мереж може бути ефективною, якщо витрати на її створення та управління будуть принаймі менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку маршрутизації інформації.

Метою роботи є отримання орієнтовної оцінки витрат на систему інформаційної безпеки типового цифрового вузла комутації при його проектуванні на етапі складання ескізного та технічного проекту. Передбачається, що комплексна система захисту інформації цифрової системи комутації створюється згідно з пакетом нормативних документів системи технічного захисту інформації (ТЗІ) на програмно-керованих АТС загального користування [2 - 16].

Цифрові системи комутації (ЦСК), як правило, оснащуються штатними і, при необхідності,