реализации определенной угрозы. В зависимости от степени детализации он может быть использован при разработке политики безопасности, проектировании профиля защиты (задания по безопасности, построении системы защиты).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Анищенко В.В., Криштофик А.М.* Базовая модель объекта информационных технологий. /Информатика № 3 (7). – Минск: ОИПИ НАН Беларуси, 2005. – С. 116-125.

2. *Анищенко В.В., Криштофик А.М.* Базовая модель системы защиты активов объекта информационных технологий. /Материалы докладов и краткие сообщения II Белорусско-российской научно-техн. конф. «Технические средства защиты информации», 17 мая-21 мая 2004, Минск-Нарочь. Доклады БГУИР. – 2004. № 5. – С. 9.

3. *Криштофик А.М., Анищенко В.В.* Управление информационной безопасностью на основе системного анализа рисков//Доклады пятой междун. конференции «Обработка информации и управление в чрезвычайных и экстремальных ситуациях». – Минск.: ОИПИ НАН Беларуси, 2006, – С.117-122.

4. *Анищенко В.В., Криштофик А.М.* Показатели защищенности информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г.- Минск: Академия управления, 2004, – С. 30-33.

5. *Криштофик А.М.* Априорная оценка потенциала атаки /Управление защитой информации, т.10 №1, 2006, Минск-Москва. – Минск.: ООО «Марфи», 2006, – С. 47-49.

6. *Криштофик А.М.* Модель комплексной оценки потенциала атаки // Материалы X междун. конференции «Комплексная защита информации». – Минск.: Амалфея, 2006, – С.111-113.

7. *Анищенко В.В., Криштофик А.М.* Использование комплексного подхода для ранжирования угроз информационной безопасности // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск. Академия управления, 2004, – С. 33-36.

А.М. Криштофик, В.В. Анищенко
Беларусь, г. Минск, ОИПИ НАН Беларуси

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Введение

Существующая нормативно-методическая база по вопросам безопасности информационных технологий (ИТ) имеет определенные недостатки. Основными из них являются: игнорирование системного подхода, как методологии построения системы защиты информации (СЗИ); отсутствие механизмов достоверного подтверждения качества и достаточности средств защиты, недостаточность проработки вопросов моделей системы защиты, системы показателей и критериев безопасности ИТ; статический подход к оценке уязвимостей [1].

Это обусловливает необходимость развития нормативно-методической базы, методик и моделей оценки защищенности на основе системного подхода.

1. Системный подход к построению системы защиты

Методология обеспечения безопасности ИС основана на концепциях анализа и управления рисками [1]. Основным недостатком существующих подходов к оценке рисков информационной безопасности (ИБ) является предположение об идеальной стойкости средств защиты.

Методологический подход к построению и оценке СЗИ с использованием системного анализа рисков основан на новых определениях остаточных уязвимостей, риска и ущерба [2]. Он предполагает проведение анализа взаимодействия элементов безопасности, характеризующих внешнюю среду, объект оценки и по-

следствия этого взаимодействия. Анализ проводится в следующей последовательности: *« угроза* (действие) ⇒ *уязвимость* (фактор) ⇒ *актив* (объект защиты) ⇒ *риск* (возможность последствий) ⇒ *ущерб* (последствия) ⇒ *контрмеры* (противодействие) ⇒ *остаточная уязвимость* (остаточный фактор) ⇒ *остаточный риск* (остаточная возможность последствий) ⇒ *остаточный ущерб* (остаточные последствия) ⇒ *достаточность защиты?»* (рис.1) [2].

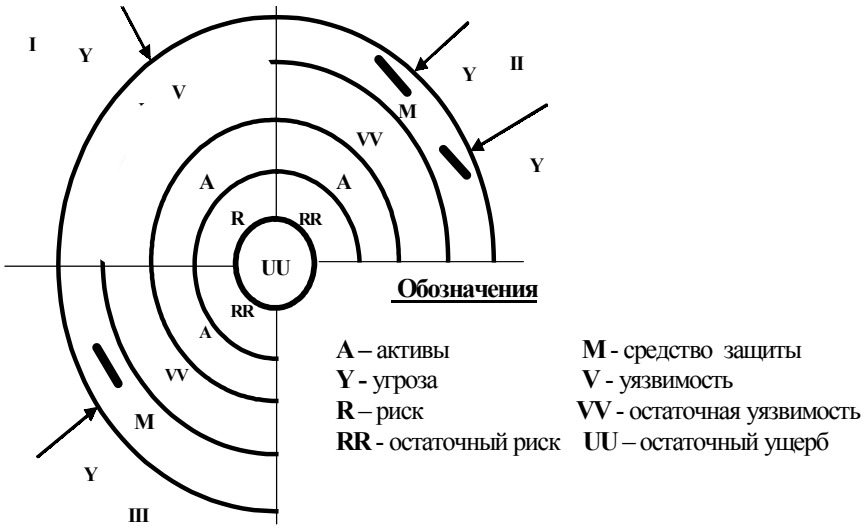

Рис. 1. Диаграмма формирования ущерба

Предполагается также, что средства защиты обладают конечной стойкостью и сами могут быть объектом реализации угроз безопасности.

В качестве показателя эффективности используется нечеткий средний ущерб от нарушения ИБ $R = \sum_{i=1}^{I} \sum_{k=1}^{K} \sum_{j=1}^{J} P_i P_{ikj} u_{ikj}$, где P_{ikj} - возможность принятия состояния нарушения информационной безопасности *ikj* при реализации угрозы $y_i \in Y = \{y_i\}, i = \overline{1,I}$ на активы $a_j \in A = \{a_j\}, j = \overline{1,J}$, используя уязвимость ИС $v_k \in V = \{v_k\}, k = \overline{1,K}$; P_i – вероятность появления угрозы y_i; u_{ikj} – максимально возможный ущерб при состоянии *ikj*.

Использование данного подхода позволило авторам разработать базовую модель ИС и подход к формированию типовых объектов оценки [2, 3], методику разработки функциональных требований безопасности [2, 3], базовую модель системы защиты с учетом ее подверженности воздействию угроз безопасности и требований безопасности, подход к классификации систем защиты [4, 5], определять необходимый состав СЗИ и предъявлять требования к их стойкости [2, 6], разрабатывать и оценивать показатели защищенности на основе анализа рисков [7] , проводить комплексную оценку и ранжирование элементов безопасности [8], предусмотреть управление рисками на протяжении всего жизненного цикла ИС [9].

Разработанная методика управления рисками информационной безопасности расширяет и дополняет концепции управления рисками, определяемые международными стандартами (рис. 2).

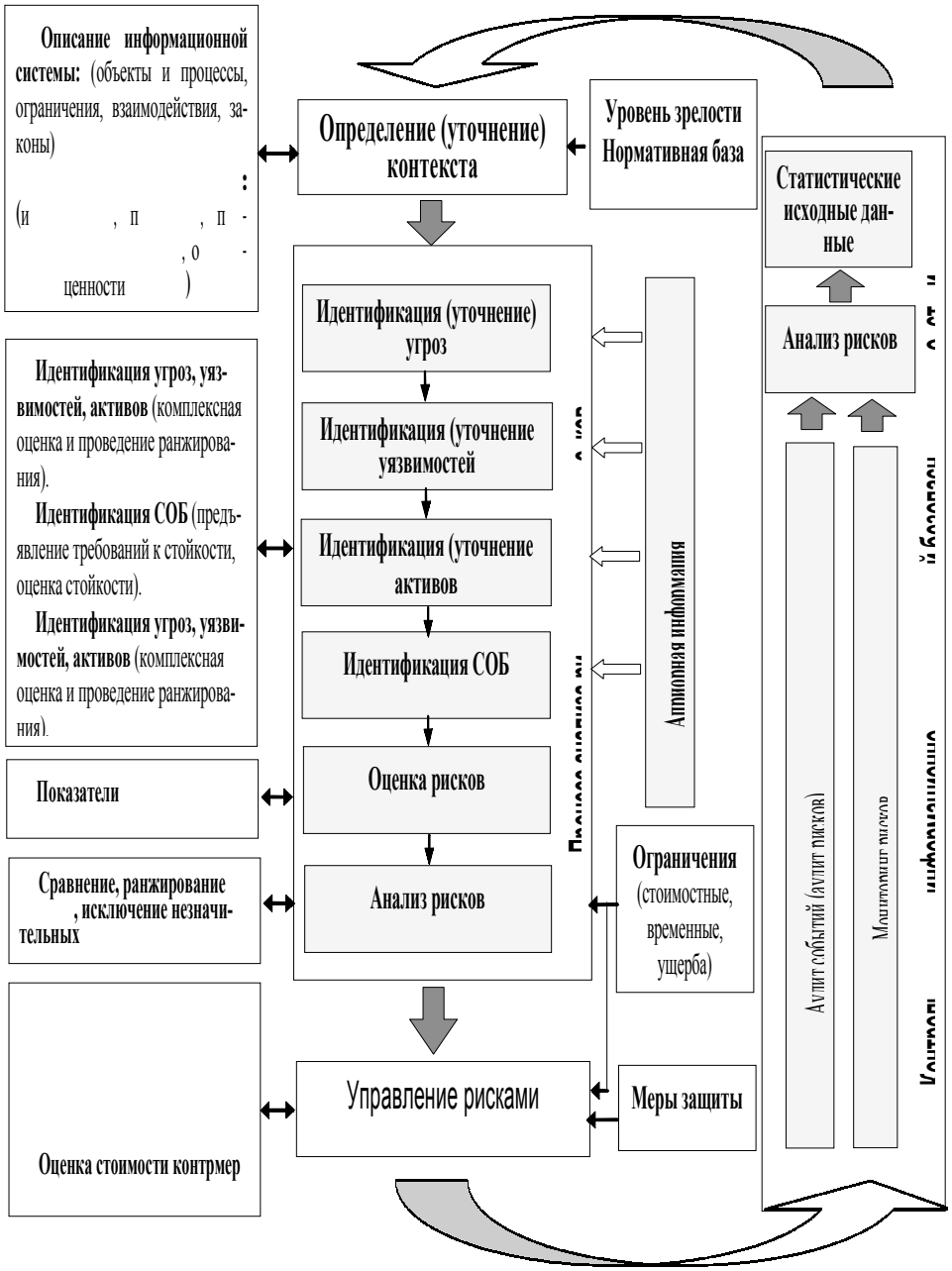

Рис. 2. Концепция управления рисками с использованием системного подхода

2. Математические модели оценки защищенности

В основу построения математических моделей оценки защищенности на различных этапах жизненного цикла положена базовая модель ИС, описываемая пятиэлементным графом взаимодействия элементов безопасности (ЭБ) $< Y, V, A, R, U >$ и определяющая негативные последствия от нарушения ИБ, характеризуемые двумя множествами [3]:

$R = Y \times V \times A = \{r_c = r_{ikj} = \langle y_i, v_k, a_j \rangle\}, c = \overline{1,C}, C = I \cdot K \cdot J$ - рисков нанесения ущерба;

$U = R \times S = \{u_c = u_{ikj}\} = \{r_c, s_j\}, c = \overline{1,C},\ j = \overline{1,J}$ - ущербов, наносимых владельцам активов вследствие реализации угроз безопасности, где s_j – оценка элемента множества ценностей активов $S = \{s_j\},\ j = \overline{1,J}$ j-го вида, для которых существует риск нанесения ущерба r_{ikj}.

Средства защиты вводятся в модель с позиций системного подхода с учетом соотношения их стоимости и возможного ущерба при условии, что существует риск нанесения ущерба и/или он превышает некоторую допустимую величину, т.е. с использованием общесистемного критерия «эффективность/стоимость» с учетом существующих ограничений (стоимостных, временных и т.д.) [5, 11]:

$$M_{треб} ::= \begin{cases} M = Y \times V = \{m_q\} = \{\langle y_i, v_k \rangle\}; \\ m_{q_{ik}} = \begin{cases} 1 & при \quad [(u_{ikj} > u_{c\,доп}) \wedge (u_{ikj} > s_{mq}) \wedge (t_{ikj} < t_{qi})]; \\ 0 & при \quad [(u_{ikj} \le u_{c\,доп}) \vee (u_{ikj} \le s_{mq}) \vee (t_{ikj} \ge t_{qi})]; \end{cases} \\ S_m = \sum\limits_q s_{m_q} \le S_{доп} \\ q \equiv ik, q = \overline{1,Q},\ Q \le I \times K, \end{cases}$$

где $u_{c\,доп}$ – порог незначительности (допустимости) ущерба; S_m , s_{m_q} - стоимость всех СЗИ и конкретного средства m_q, соответственно; $S_{доп}$ - ограничения на стоимость СЗИ; 1, 0 – значения истинности и ложности высказывания «наличие элемента множества СЗИ», характеризующие наличие и отсутствие элемента m_q; t_{ikj}, t_{qi} - время реализации угрозы по пути $\boldsymbol{i \to k \to j}$ и время реакции СЗИ m_q по перекрытию пути воздействия угрозы, соответственно.

Это приводит к изменению структуры и характеристик ИС и, как следствие, появлению множеств остаточных уязвимостей, рисков и ущербов. Остаточные уязвимости определены с учетом стойкости СЗИ (рис.3).

Это приводит к изменению базовой модели, которая переходит в модель системы защиты. Модель системы защиты представляется шестиэлементным графом взаимодействия ЭБ $< Y, M, V, A, R^{\otimes}, U^{\otimes} >$ [12].

Учитывая тот факт, что СЗИ, как подсистема ОО, также является объектом осуществления угроз безопасности, разработана модель учета уязвимостей СЗИ (рис. 4), и на ее основе модель системы защиты с учетом уязвимостей СЗИ [13].

Отличительной особенностью разработанных моделей, кроме учета стойкости СЗИ и их собственных уязвимостей, является одновременное использование двух характеристик нечетких случайных величин, описывающих процесс нанесения ущерба.

Элементы множеств, описывающих взаимодействие ОО с внешней средой являются нечеткими случайными величинами $K = (k, \mu(k))$, где k - оценочное значение соответствующего коэффициента, $\mu(k)$ - нечеткая составляющая (функция принадлежности) нечеткой величины k.

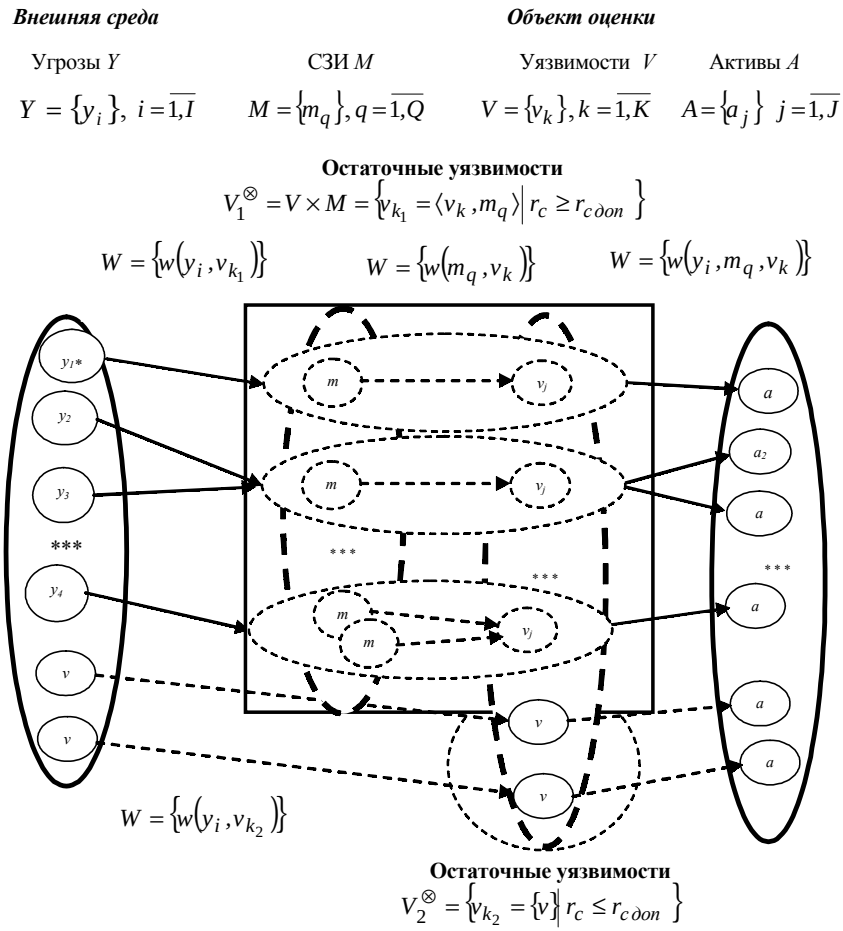

Рис.3. Определение остаточной уязвимости

В зависимости от способа описания оценочного значения соответствующего коэффициента - среднее значение или плотность распределения нечеткой случайной величины *k*, возможны два подхода к оценке состояний нарушения безопасности ОО:

- нечеткое описание процесса нарушения ИБ;
- описание процесса нарушения безопасности с использованием нечетких случайных величин.

При нечетком описании процесса нарушения ИБ для оценки показателей защищенности используются специальные операции суммирования нечетких величин, при которых суммирование элементов-носителей является скалярным, а значение функции принадлежности вычисляется согласно правилу центра тяжести, используемого в операции дефазификации, т.е. с использованием свертки нечетких весов. При втором способе описания элементов безопасности оценка показателей защищенности выполняется с использованием вероятности нечеткого случайного события.

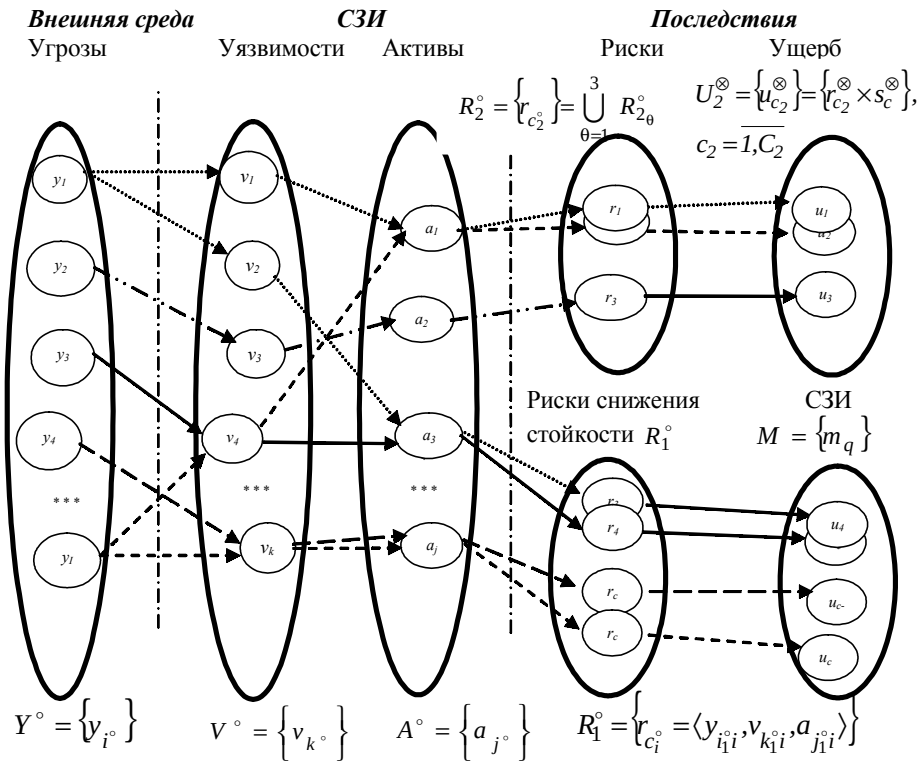

Рис. 4. Модель учета уязвимостей СЗИ

Заключение

Рассмотрен важный в методическом и прикладном плане вопрос оценки защищенности ИС. Предложенный методологический подход и разработанные на его основе модели основаны на системном подходе, предусматривающем проведение оценки негативных последствий от нарушения ИБ на основе анализа изменения состава и структуры ИС при его взаимодействии с внешней средой. Он расширяет и дополняет концепции управления рисками, определяемые международными стандартами, определяющими базовые и повышенные требования безопасности за счет учета стойкости СЗИ и их подверженности воздействию угроз безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Криштофик А.М.* Нормативно-методическая база в области информационной безопасности. Состояние и перспективы развития // Информатика № 3 (11). – Минск.: ОИПИ НАН Беларуси, 2006, – С.101-111.

2. *Анищенко В.В., Криштофик А.М.* Актуальные вопросы оценки защищенности информационных систем военного назначения // Наука и военная безопасность. № 1, С.30-34. – Минск.: МО РБ, 2005.

3. *Анищенко В.В., Криштофик А. М.* Базовая модель объекта информационных технологий // Информатика № 3 (7). – Минск: ОИПИ НАН Беларуси, 2005. – С.116-125.

4. *Анищенко В.В., Криштофик А. М.* Разработка функциональных требований безопасности к высокопроизводительным вычислительным системам на основе анализа рисков / Доклады Международной научной конференции «Суперкомпьютерные системы и их при-

менение» SSA'2004, 26-28 октября 2004 г., Минск, – Минск.: ОИПИ НАН Беларуси, 2004, – С. 238-243.

5. *Анищенко В.В., Криштофик А. М.* Базовая модель системы защиты активов объекта информационных технологий // Материалы докладов и краткие сообщения II Белорусско-российской научно-техн. конф. «Технические средства защиты информации», 17 мая-21 мая 2004, Минск-Нарочь. Доклады БГУИР. –2004. № 5. – С. 9.

6. *Анищенко В.В., Криштофик А. М.* Влияние уязвимостей средств защиты на безопасность объектов информационных технологий // Материалы IX Международной конференции «Комплексная защита информации», 1-3 марта 2005 г., Раубичи (Беларусь). – Минск: ОИПИ НАН Беларуси, 2005, – С.52-54.

7. *Анищенко В.В., Криштофик А. М.* Методика оценки защищенности автоматизированных систем при повышенных требованиях безопасности // Тезисы докладов Международной научной конференции по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения. – Минск: БелИСА, 2005, – С. 150-151

8. *Анищенко В.В., Криштофик А.М.* Показатели защищенности информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск: Академия управления, 2004, – С. 30-33

9. *Анищенко В.В., Криштофик А.М.* Комплексный подход к ранжированию уязвимостей информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск: Академия управления, 2004, –С. 36-39.

10. *Анищенко В.В., Криштофик А.М.* Этапы проведения оценки защищенности объектов информационных технологий // Материалы IX Международной конференции «Комплексная защита информации», 1-3 марта 2005 г., Раубичи (Беларусь). – Минск: ОИПИ НАН Беларуси, 2005, – С55-57.

11. *Криштофик А.М., Анищенко В.В.* Управление информационной безопасностью на основе системного анализа рисков//Доклады пятой междун. конференции «Обработка информации и управление в чрезвычайных и экстремальных ситуациях». – Минск: ОИПИ НАН Беларуси, 2006, – С.117-122.

12. *Криштофик А.М.* Модель комплексной оценки потенциала атаки // Материалы X междун. конференции «Комплексная защита информации». – Мн.: Амалфея, 2006, – С.111-113

13. *Криштофик А.М.* Модель оценки уязвимости системы защиты информации //Материалы третьей междун. конференции «Информационные системы и технологии», IST'2006. – Минск: Академия управления при Президенте РБ, 2006. – С.109 -114.

И.В. Машкина
Россия, г. Уфа, УГАТУ

ПОДСИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОМУ УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ

Для успешного использования современных информационных технологий необходимо *эффективное управление* не только сетью, но и системой защиты информации (СЗИ). В число задач управления защитой информации (ЗИ) входит обеспечение работы проектной группы приложений: определение *модульного состава* и *точек установки* средств защиты (СрЗ) в сети предприятия [1].

Это обусловлено тем, что защита информации – это не разовое мероприятие и не совокупность средств защиты, а непрерывный *целенаправленный процесс*, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы (ИС). При этом важными аспектами обеспечения безопасности информации являются принципы комплексности, гибкости системы