Ю.С. Лунёв

ИССЛЕДОВАНИЕ ВЗАИМООТНОШЕНИЙ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ОВД В ПРОЦЕССЕ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

RESEARCH OF RELATIONSHIPS IN DISTRIBUTED INFORMATION SYSTEMS IN RUSSIA MILITIA IN PROTECTING AGAINST MALICIOUS SOFTWARE

Рассматривается моделирование действий вредоносных программ в распределённых информационных системах с помощью методов теории конфликта.

This article is devoted to the modeling action Malware distribution of information systems using the conflict theory.

Современные информационные системы ОВД построены, как правило, как распределённые информационные системы (РИС), что позволяет увеличить оперативность обмена информацией и, тем самым, способствует повышению эффективности профессиональной деятельности сотрудников ОВД.

В распределённых информационных системах существенно возрастает количество потенциальных угроз информационной безопасности, в том числе и со стороны действия вредоносных программ.

По определению рекомендаций по стандартизации Р 50.1.056-2005, вредоносная программа — это программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы [1]. В указанных рекомендациях даны определения и таким понятиям, как «компьютерный вирус» и «программная закладка», которые в нашем исследовании мы будем понимать под вредоносной программой. Единственное, что объединяет все перечисленные типы вредоносных программ — это цели, с которыми они создаются. Можно выделить две основные группы целей:

1) отбор в процессе своего функционирования аппаратных ресурсов РИС (оперативной и постоянной памяти, процессорного времени);

2) нанесение ущерба только информационной подсистеме РИС (изменение, уничтожение, кража информации).

В соответствии с этим будем выделять два подмножества вредоносных программ:

- вредоносные программы 1-го типа — *ВП-1*, преимущественно направленные на достижение целей из первой группы;

- вредоносные программы 2-го типа — *ВП-2*, преимущественно направленные на достижение целей из второй группы.

Аппаратные возможности современной компьютерной техники постоянно возрастают. Воздействие вредоносных программ первого типа становится существенным лишь спустя некоторое время. При разумном подходе к осуществлению политики информационной безопасности своевременно назначаются профилактические работы, которые обеспечивают устранение действий этих вредоносных программ.

Учитывая специфику органов внутренних дел, и в частности высокую социальную значимость обрабатываемой в РИС ОВД информации и опасность её разглашения

или утери, следует считать недопустимым наличие в памяти компьютера вредоносных программ второго типа.

Чтобы снизить риск потерь от воздействия вредоносных программ в РИС, создаётся специальная система защиты информации (СЗИ), которая обеспечивает непрерывное осуществление политики информационной безопасности в части борьбы с вредоносными программами. Основным методом работы СЗИ является периодическое проведение профилактических мероприятий по выявлению, устранению и диагностике вредоносных программ, как правило, с полной или частичной приостановкой работы информационной системы или её элементов. К таким мероприятиям, в частности, относятся:

- постоянный мониторинг и защита от действий вредоносных программ;
- сканирование на наличие вредоносных программ.

Таким образом, можно считать, что РИС включает две подсистемы:

- пользовательскую систему (ПС), осуществляющую все функции, связанные с обеспечением работы пользователей;
- систему защиты информации (СЗИ), осуществляющую перечисленные выше функции борьбы с вредоносными программами.

Обратимся к описанию перечисленных элементов.

С этой целью определим множества потенциальных состояний, в которых могут находиться элементы и условия перехода элементов из состояния в состояние.

Современные операционные системы и системы защиты информации, как правило, проводят постоянный мониторинг вредоносных программ во время работы пользователей. Однако это не обеспечивает полной безопасности работы элементов ПС. Поэтому периодически необходимо производить профилактические работы по выявлению, устранению и диагностике вредоносных программ с приостановкой работы пользователей.

В связи с этим целесообразно выделить состояния программного обеспечения СЗИ, обеспечивающего работу данного элемента ПС:

ω_1 — эффективный мониторинг вредоносных программ,

ω_2 — неэффективный мониторинг вредоносных программ,

ω_3 — профилактика вредоносных программ с приостановкой работы пользователей.

Переход из одного состояния в другое осуществляется:

- либо при инициализации вредоносной программы, не выявленной в ходе мониторинга,
- либо в соответствии с командами на начало и завершение выполнения профилактических работ программным обеспечением СЗИ.

Возможные варианты перехода программного обеспечения СЗИ из состояния в состояние показаны на рис.1.

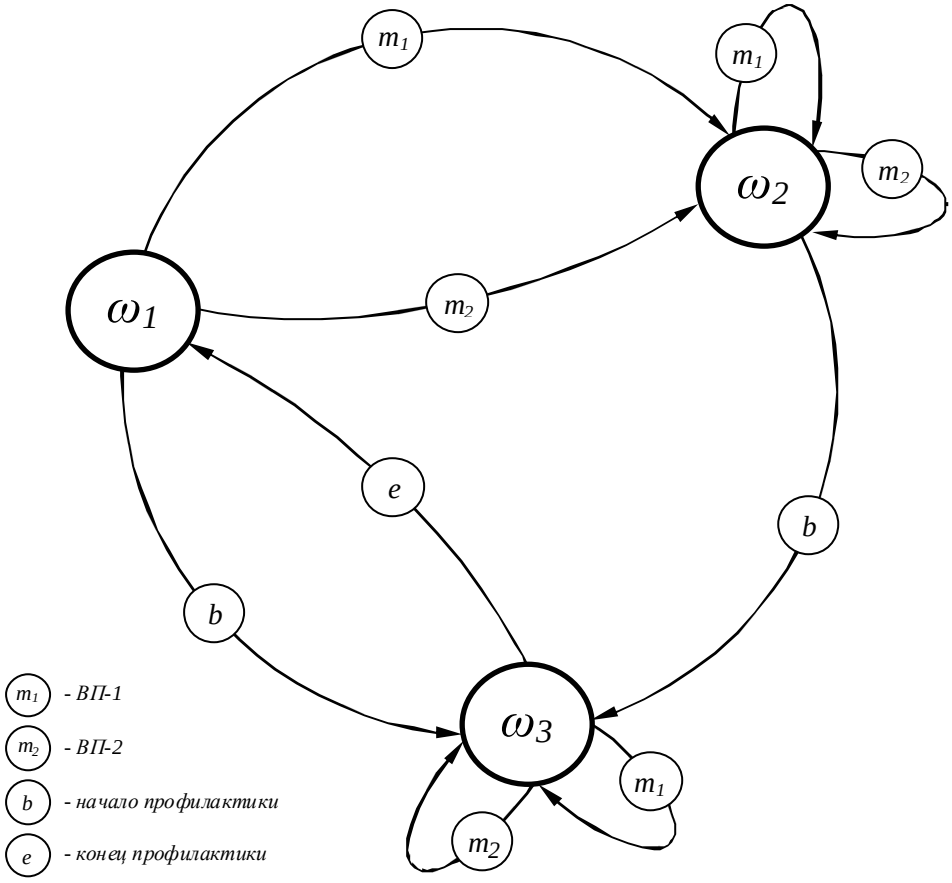

Рис.1. Состояния функционирования программного обеспечения СЗИ

После выполнения профилактических работ элемент ПС функционирует в нормальном режиме. Однако через некоторое время могут внедриться вредоносные программы, не выявленные в результате мониторинга, и элемент ПС начинает работать в потенциально опасном режиме, когда может быть нанесён ущерб информации или аппаратным ресурсам элемента ПС.

Следовательно, в каждый момент времени элементы ПС могут находиться в каком-либо одном из возможных состояний:

χ_1 — работа в нормальном режиме,

χ_2 — работа в потенциально опасном режиме при наличии в памяти компьютера вредоносных программ только первого типа,

χ_3 — работа в потенциально опасном режиме при заметности вредоносного воздействия вредоносных программ только первого типа,

χ_4 — работа в потенциально опасном режиме при наличии в памяти компьютера вредоносных программ второго типа,

χ_5 — приостановка работы для осуществления профилактики.

Переход из одного состояния в другое осуществляется:

- либо при инициализации вредоносной программы первого или второго типов,

- либо в соответствии с командами на начало и завершение выполнения профилактических работ программным обеспечением СЗИ.

Возможные варианты перехода элемента ПС из состояния в состояние показаны на рис. 2.

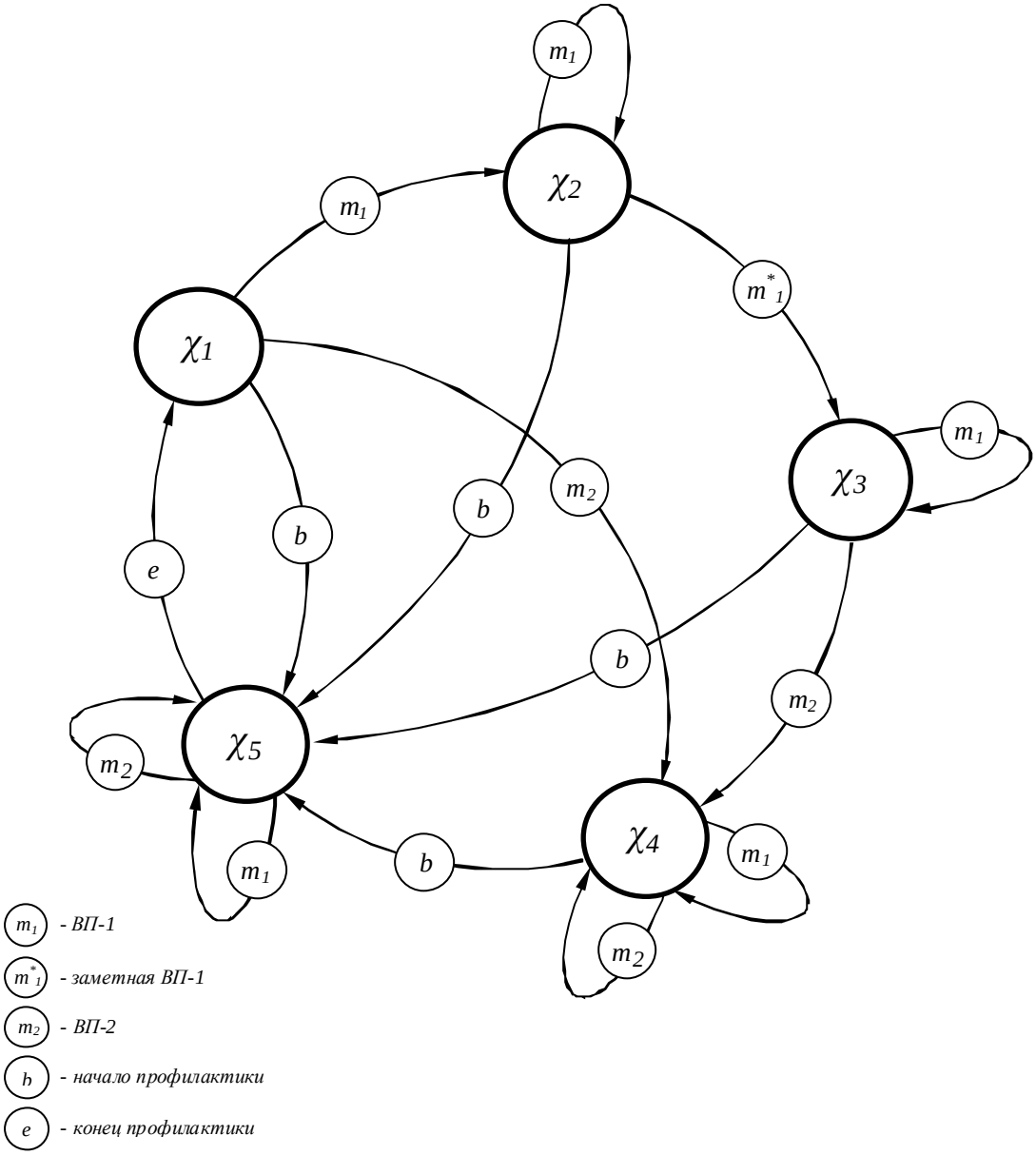

Рис. 2. Возможные варианты смены состояний элемента ПС

Вредоносные программы, относящиеся к первому и второму типам, различаются функционированием по достижению цели, поэтому опишем их раздельно.

Функционирование вредоносных программ первого типа на элементе ПС последовательно проходят 2 стадии. Первая осуществляется параллельно с работой пользователей. Занимая ресурсы памяти и процессора, они снижают эффективность работы элемента ПС. На второй стадии вредоносные программы работают одновременно с программным обеспечением СЗИ, осуществляющим профилактику, в этот момент работа пользователей полностью приостановлена, и их эффективность работы — наименьшая. После окончания профилактики определённое время программы отсутствуют и не снижают эффективность работы пользователей.

Таким образом, программы, относящиеся к первому типу, могут находиться в трех состояниях (рис 3):

φ_1 — состояние отсутствия в памяти элемента ПС;

φ_2 — состояние отбора ресурсов у пользователя элемента ПС непосредственно;

φ_3 — состояние отбора ресурсов у пользователя элемента ПС посредством СЗИ.

Переход из одного состояния в другое осуществляется:

- либо при инициализации вредоносной программы, не выявленной в ходе мониторинга,

- либо в соответствии с командами на начало и завершение выполнения профилактических работ программным обеспечением СЗИ.

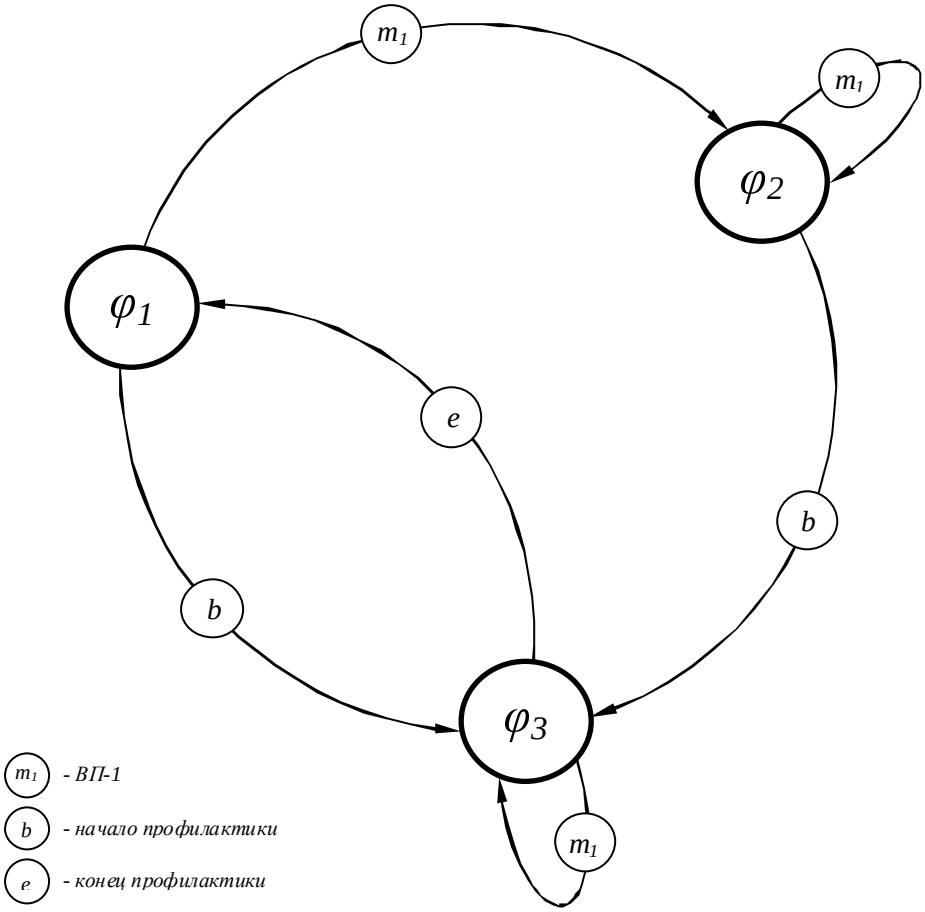

Рис. 3. Возможные варианты смены состояний вредоносных программ первого типа

Функционирование вредоносных программ второго типа на элементе ПС осуществляется только параллельно с работой пользователей. Именно в этот период времени он может нанести ущерб информационной подсистеме РИС. Будем считать, что во время осуществления профилактики вредоносные программы второго типа не имеют возможности нанесения ущерба информационной подсистеме.

Таким образом, программы, относящиеся ко второму типу, могут находиться в двух состояниях (рис. 4):

- ψ_1 — состояние отсутствия в памяти элемента ПС;

- ψ_2 — состояние возможности нанесения ущерба информационной подсистеме РИС.

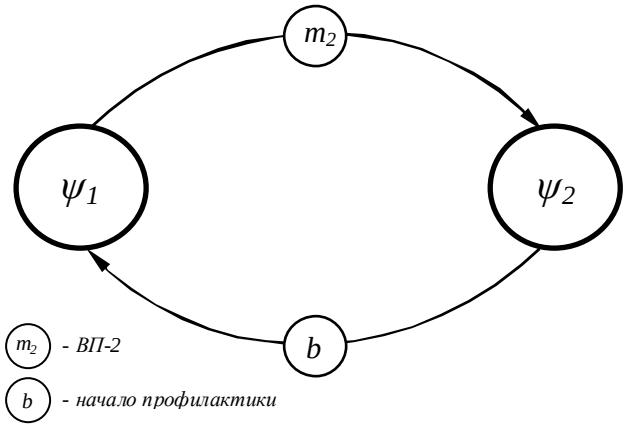

Рис. 4. Возможные варианты смены состояний вредоносных программ второго типа

Исследование взаимоотношений элементов систем осуществляется на основе анализа значений функций полезности этих элементов [2].

Обозначим:

τ_{si} — множество промежутков времени нахождения соответствующего элемента в состоянии $s_i \in \{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \omega_1, \omega_2, \omega_3, \varphi_1, \varphi_2, \varphi_3, \psi_1, \psi_2\}$;

$P_i^{\alpha}(t)$ — функцию полезности объекта α

Функционирование элемента пользовательской системы будем считать эффективным, если он находится в состояниях χ_1 или χ_2:

$$P_i^{Эл.ПС}(t) = \begin{cases} 1, если & t \in \tau_{\chi 1} \cup \tau_{\chi 2} \\ 0, если & t \in \tau_{\chi 3} \cup \tau_{\chi 4} \cup \tau_{\chi 5} \end{cases}.$$

Функционирование элемента системы защиты информации будем считать эффективным, если она находится в состояниях ω_1 или ω_3:

$$P_i^{Ýë.ÑÇÈ}(t) = \begin{cases} 1, åñëè & t \in \tau_{\omega 1} \cup \tau_{\omega 3} \\ 0, åñëè & t \in \tau_{\omega 2} \end{cases}.$$

Функционирование вредоносной программы первого типа будем считать эффективным, если она находится в состояниях φ_2 или φ_3:

$$P_i^{ВП-1}(t) = \begin{cases} 1, если & t \in \tau_{\varphi 2} \cup \tau_{\varphi 3} \\ 0, если & t \in \tau_{\varphi 3} \cup \tau_{\varphi 4} \end{cases}.$$

Функционирование вредоносной программы первого типа будем считать эффективным, если она находится только в состоянии ψ_2:

$$P_i^{ВП-2}(t) = \begin{cases} 1, если & t \in \tau_{\psi 2} \\ 0, если & t \in \tau_{\psi 1} \end{cases}.$$

Вариант изменения значений функций полезности за период τ между двумя последовательными приостановками работы для осуществления профилактики приведён на рис. 5.

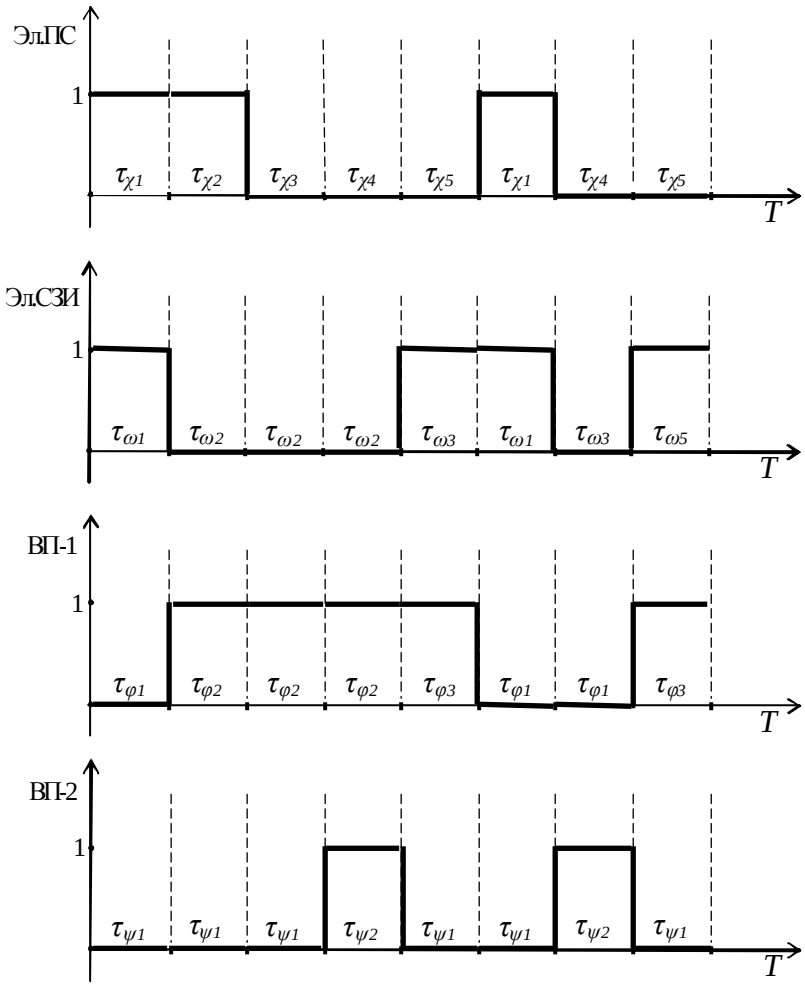

Рис. 5. Основные варианты изменения функций полезности рассматриваемых элементов

Анализ изменения функций полезности позволяет определить тип взаимоотношения между элементами:

- если возрастание функции полезности элемента *A* приводит к убыванию функции полезности элемента *B*, то имеет место отношение конфликта между *A* и *B*: $A \blacktriangleright B$;

- если возрастание или убывание функции полезности элемента *A* не влияет на функции полезности элемента *B*, то имеет место отношение безразличия между *A* и *B*: $A \blacktriangleright_0 B$;

- если возрастание функции полезности элемента *A* приводит к возрастанию функции полезности элемента *B*, то имеет место отношение согласия между *A* и *B*: $A \blacktriangleright_c B$.

С учётом всех возможных вариантов можно сделать следующие основные выводы:

- элементы ПС и СЗИ могут находиться как в отношении согласия (например, при эффективном мониторинге вредоносных программ), так и в отношении конфликта (например, при приостановке работы пользователя для проведения профилактики);

- элементы ПС и вредоносные программы второго типа находятся только в отношении конфликта;

- элементы ПС и вредоносные программы первого типа могут находиться как в отношении конфликта, так и в отношении безразличия.

Полный перечень отношений приведён на рис. 6.

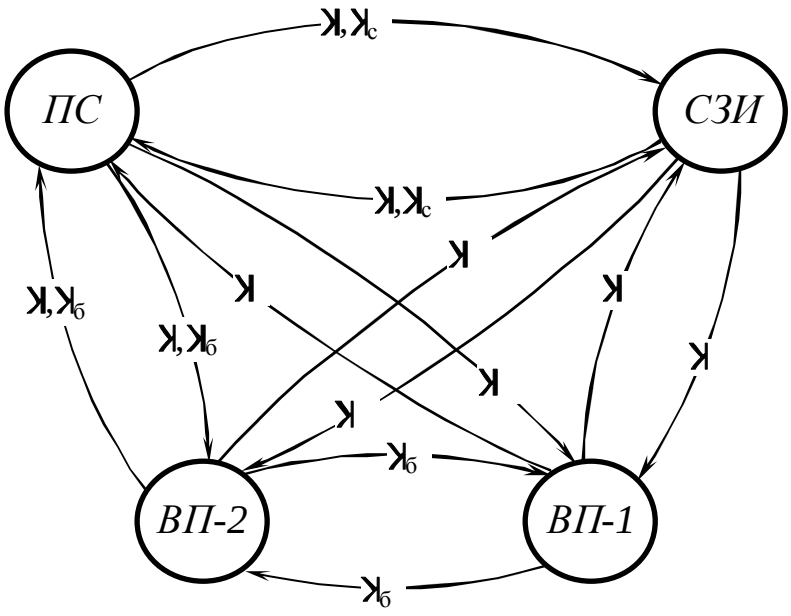

Рис. 6. Представление взаимоотношений между элементами системы в виде ориентированного графа

Полученные результаты могут быть использованы при определении политики информационной безопасности в РИС ОВД.

ЛИТЕРАТУРА

1. Р 50.1.056-2005 — «Информационные технологии. Основные термины и определения в области технической защиты информации».

2. Сысоев В.В. Конфликт. Сотрудничество. Независимость. системное взаимодействие в структурно-параметрическом представлении / В.В. Сысоев. — М.: Московская академия экономики и права, 1999. — 151 с.

3. Новосельцев В.И. Системная конфликтология / В.И. Новосельцев. — Воронеж: Кварта, 2001.