УДК 004.056

**А.А. Конев**

# Подход к построению модели угроз защищаемой информации

Предложен подход к построению модели угроз, основанный на использовании схемы информационных процессов. Информационные процессы построены с учетом действий с защищаемой информацией и среды ее распространения. При этом учитывается преобразование формы представления информации при переходе из одной среды в другую.
**Ключевые слова:** информационная безопасность, модель угроз, информационный процесс.

Построение модели угроз является одним из обязательных этапов предпроектного обследования. При этом под моделью угроз чаще всего понимают перечень угроз для конкретной информационной системы [1]. Данная работа посвящена описанию подхода к построению формализованного представления модели угроз, на основе которого будет конкретизироваться перечень угроз информационной системы.

Основное отличие предлагаемого подхода заключается в использовании в качестве базиса перечня информационных процессов, происходящих с защищаемой информацией. Выделены три информационных процесса: хранение, обработка и доставка. При этом возможно вовлечение в процесс передачи информации двух информационных процессов, связанных с обработкой (рис. 1).

Переходы между состояниями хранение и обработка – выдача хранимого носителя информации или документа и сдача его на хранение, между обработками в двух средах – чтение и запись, между обработкой и доставкой – отправка и получение информации, представленной в формате для пересылки (сетевой пакет, пакет бумажных документов, пересылаемый по почте и др.).

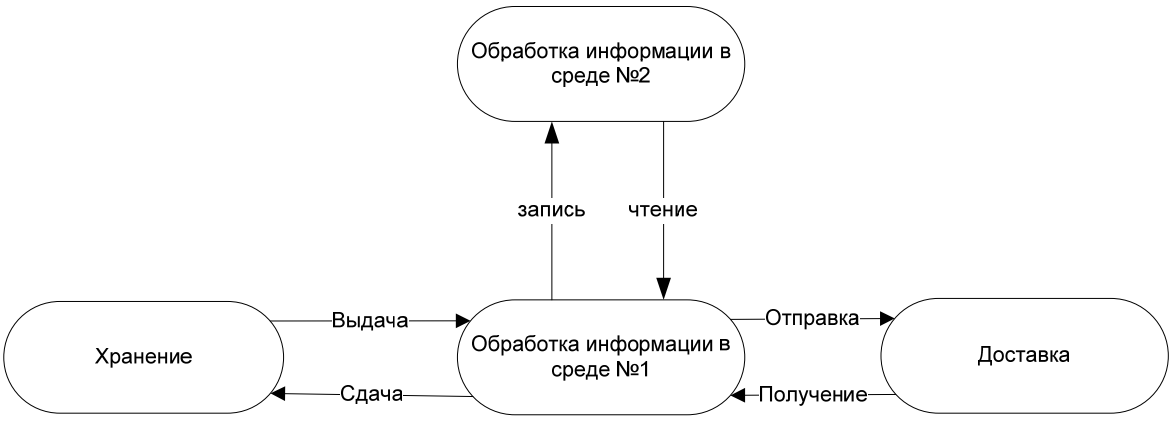


Рис. 1. Типовая схема информационных процессов

В предлагаемом подходе классификация сред распространения информации отличается от классификации, приведенной в модели угроз ФСТЭК [2]. Предлагается учитывать следующие среды: визуальную, акустическую, виртуальную (байты, протоколы и т.п.), сигналы, физическую.

В подходе вводится дополнительная физическая среда, в нее входит представление информации на физическом носителе. Физическим носителем может являться, например, компакт-диск, жесткий диск, USB-накопитель, аудиокассета, видеокассета. Информация на такой носитель записывается в виде сигналов, но в случае отключения носителя от устройства, в котором оно используется, носитель становится статическим объектом, не передающим и не принимающим сигналы. Таким образом, стоит учитывать не только те угрозы, которые применимы к подключенному носителю, а еще и угрозы, относящиеся к носителю как к физическому объекту. Это такие угрозы, как, например, хищение носителя, нарушение его целостности и др.

На основе данной типовой схемы были построены ее частные случаи – схема информационных процессов с физическим доступом (рис. 2), схема информационных процессов с использованием средств автоматизации (рис. 3) и схема информационных процессов без использования средств автоматизации (рис. 4). В разработанной модели угроз под видом представления информации подразумевается совокупность состояния (хранение, обработка, доставка) и среды.

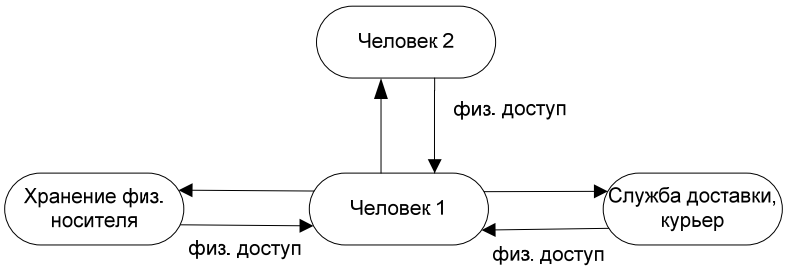


Рис. 2. Схема информационных процессов с физическим доступом

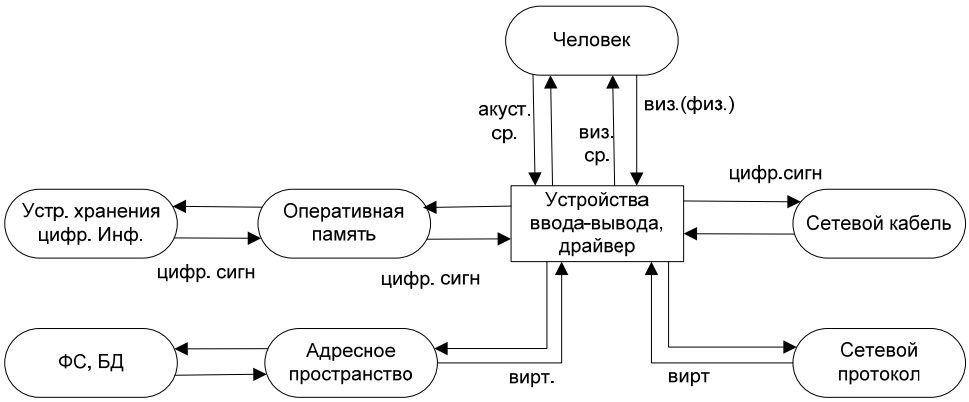


Рис. 3. Схема информационных процессов с использованием средств автоматизации

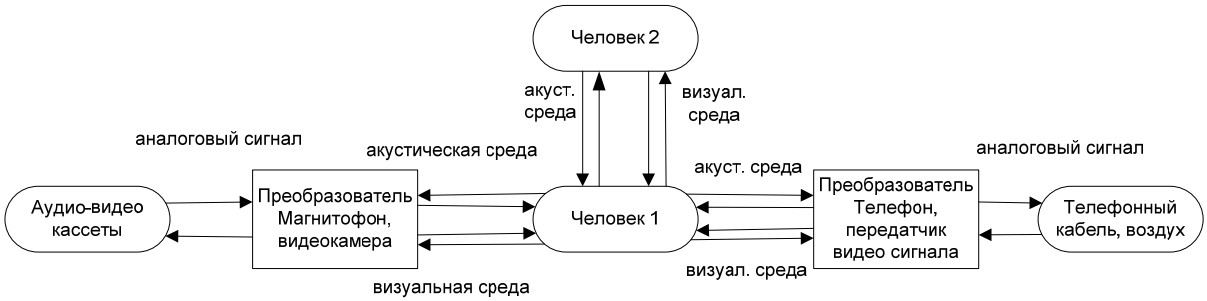


Рис. 4. Схема информационных процессов без использования средств автоматизации

Для каждой среды были определены возможные носители информации (табл. 1).

Устройства хранения цифровой и аналоговой информации являются физическими объектами, поэтому далее эти пункты будут объединены в хранении физической среды.

Таблица 1

**Возможные носители в каждой среде**

| Условное обозначение | Среда | Состояние | Возможные носители |
|---|---|---|---|
| $F_s$ | Физическая | Хранение | Жесткий диск, USB-накопители, аудио-видеокассеты, бумажный носитель |
| $Vr_s$ | Виртуальная | Хранение | Файловая система, база данных |
| $F_p$ | Физическая | Обработка | Жесткий диск, USB-накопители, аудио-видеокассеты, бумажный носитель |
| $Vz_p$ | Визуальная | Обработка | Человек, бумажный носитель |
| $A_p$ | Акустическая | Обработка | Человек |
| $Vr_p$ | Виртуальная | Обработка | Адресное пространство |
| $S_d$ | Сигналы | Доставка | Сетевой кабель, воздух |
| $F_d$ | Физическая | Доставка | Жесткий диск, USB-накопители, аудио-видеокассеты, бумажный носитель |
| $Vr_d$ | Виртуальная | Доставка | Сетевой протокол |

Бумажный носитель относится к физической среде, т.к. к нему применимо физическое воздействие. При этом в отличие от других физических носителей, бумажный носитель используется в визуальной среде, т.к. на нем можно хранить информацию, доступную для человека без использования дополнительных преобразователей.

Для построения общего графа был проработан полный список возможных переходов. В ходе работы были проанализированы все переходы между состояниями и были выделены все переходы, которые могут быть осуществлены. Связи представлены в виде матрицы смежности (табл. 2).

Таблица 2

**Матрица смежности для переходов**

| | $F_s$ | $Vr_s$ | $F_p$ | $Vz_p$ | $A_p$ | $Vr_p$ | $S_d$ | $F_d$ | $Vr_d$ |
|---|---|---|---|---|---|---|---|---|---|
| $F_s$ | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| $Vr_s$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| $F_p$ | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| $Vz_p$ | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| $A_p$ | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| $Vr_p$ | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| $S_d$ | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| $F_d$ | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| $Vr_d$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |

Обозначения: 0 – связь невозможна; 1 – связь возможна.

Переходы из табл. 2, в которых информация меняет форму своего представления, осуществляются с помощью преобразователей. Все эти переходы и преобразователи, через которые они осуществляются, приведены в табл. 3.

Во всех случаях использования преобразователей для изменения вида представления информации, приведенных в табл. 3, имеется переход в среду сигналов через побочные электромагнитные излучения и наводки. Это приводит к появлению дополнительных угроз конфиденциальности и целостности.

Таблица 3

**Возможные преобразователи при переходе между средами**

| Состояние в рамках среды 1 | Состояние в рамках среды 2 | Возможные преобразователи |
|---|---|---|
| $F_s$ | $Vz_p$ | Видеокамера, видеопроигрыватель |
| $F_s$ | $A_p$ | Магнитофон, диктофон |
| $F_s$ | $Vr_p$ | Контроллер, порты |
| $Vr_p$ | $Vz_p$ | Веб-камера, монитор, принтер |
| $Vr_p$ | $A_p$ | Динамик, микрофон, вибродатчик |
| $S_d$ | $Vr_p$ | Сетевая карта |
| $S_d$ | $A_p$ | Телефон |
| $S_d$ | $Vz_p$ | Устройства передачи видеосигнала |

На основе матрицы смежности, приведенной в табл. 2, была построена общая схема информационных процессов (рис. 5).

На рис. 5 в овальных фигурах изображены состояния в каждой среде, прямоугольными блоками изображены преобразователи. Замыкание переходов из блоков с физической обработкой, визуальной обработкой и акустической обработкой в те же самые блоки означает переход в рамках одной среды и одного состояния на другой носитель информации. На основе схемы информационных процессов построен граф переходов (рис. 6).

При построении модели угроз, как и в модели угроз безопасности ФСТЭК, было выделено три основных типа угроз: угрозы конфиденциальности, угрозы целостности, угрозы доступности.

Но в отличие от модели угроз ФСТЭК вводится дополнительная классификация угроз.

Классы угроз конфиденциальности: 1) подмена получателя в состоянии среды №1; 2) подмена получателя в состоянии среды №2; 3) подмена канала; 4) контроль канала.

Классы угроз целостности: 1) подмена отправителя в состоянии среды №1; 2) подмена отправителя в состоянии среды №2; 3) подмена канала; 4) воздействие на канал.

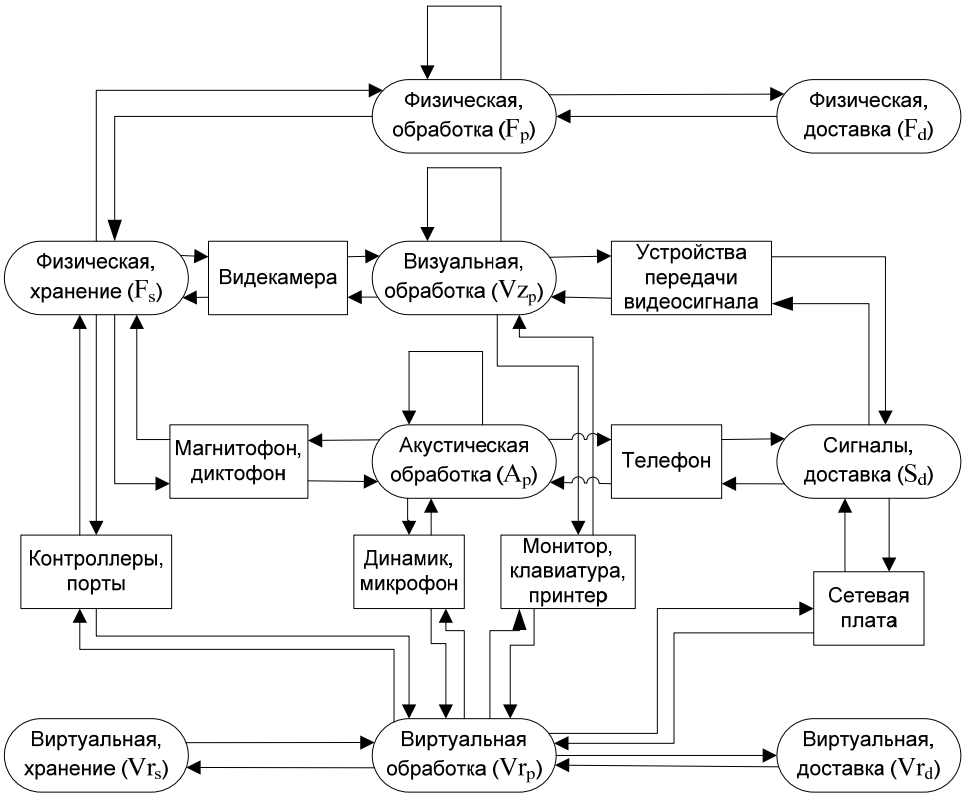


Рис. 5. Общая схема информационных процессов

Классы угроз доступности: 1) недоступность носителя в состоянии среды №1; 2) недоступность носителя в состоянии среды №2; 3) нарушения канала передачи; 4) недоступность преобразователя.

Класс угроз конфиденциальности «контроль канала» и класс угроз целостности «воздействие на канал» не существуют в случае перехода, происходящего в физической среде. Угрозы доступности не существуют в случае перехода в рамках одного состояния, одной среды.

В итоге было разработано формализованное представление модели угроз. Формализованное представление основано на использовании следующих множеств: 1) множество состояний в рамках среды; 2) множество возможных переходов; 3) множество типов угроз; 4) множество классов угроз.

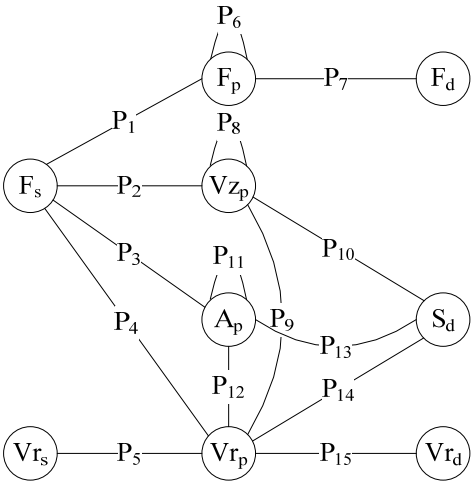


Рис. 6. Граф переходов

Все возможные состояния приведены в табл. 1. В информационном процессе участвуют два состояния в одной или разных средах. Обозначим множество состояний первой среды – $Q$, а множество состояний второй среды, участвующей в информационном процессе, – $W$. Множества $Q$ и $W$ будут эквивалентными (множество $W$ состоит из тех же элементов, что и множество $Q$).

Множество состояний в первой среде:

$$Q = \{F_s, Vr_s, F_p, Vz_p, A_p, Vr_p, S_d, F_d, Vr_d\}.$$

Множество состояний во второй среде:

$$W = \{F_s, Vr_s, F_p, Vz_p, A_p, Vr_p, S_d, F_d, Vr_d\}.$$

Для того чтобы получить множество всех возможных переходов из одного состояния в другое, необходимо произвести декартово перемножение множеств $Q$ и $W$:

$Q \times W = \{(F_s, F_s), (F_s, Vr_s), (F_s, F_p), (F_s, Vz_p), (F_s, A_p), (F_s, Vr_p), (F_s, S_d), (F_s, F_d), (F_s, Vr_d), (Vr_s, F_s), (Vr_s, Vr_s), (Vr_s, F_p), (Vr_s, Vz_p), (Vr_s, A_p), (Vr_s, Vr_p), (Vr_s, S_d), (Vr_s, F_d), (Vr_s, Vr_d), (F_p, F_s), (F_p, Vr_s), (F_p, F_p), (F_p, Vz_p), (F_p, A_p), (F_p, Vr_p), (F_p, S_d), (F_p, F_d), (F_p, Vr_d), (Vz_p, F_s), (Vz_p, Vr_s), (Vz_p, F_p), (Vz_p, Vz_p), (Vz_p, A_p),$

$(Vz_p, Vr_p)$, $(Vz_p, S_d)$, $(Vz_p, F_d)$, $(Vz_p, Vr_d)$, $(A_p, F_s)$, $(A_p, Vr_s)$, $(A_p, F_p)$, $(A_p, Vz_p)$, $(A_p, A_p)$, $(A_p, Vr_p)$, $(A_p, S_d)$, $(A_p, F_d)$, $(A_p, Vr_d)$, $(Vr_p, F_s)$, $(Vr_p, Vr_s)$, $(Vr_p, F_p)$, $(Vr_p, Vz_p)$, $(Vr_p, A_p)$, $(Vr_p, Vr_p)$, $(Vr_p, S_d)$, $(Vr_p, F_d)$, $(Vr_p, Vr_d)$, $(S_d, F_s)$, $(S_d, Vr_s)$, $(S_d, F_p)$, $(S_d, Vz_p)$, $(S_d, A_p)$, $(S_d, Vr_p)$, $(S_d, S_d)$, $(S_d, F_d)$, $(S_d, Vr_d)$, $(F_d, F_s)$, $(F_d, Vr_s)$, $(F_d, F_p)$, $(F_d, Vz_p)$, $(F_d, A_p)$, $(F_d, Vr_p)$, $(F_d, S_d)$, $(F_d, F_d)$, $(F_d, Vr_d)$, $(Vr_d, F_s)$, $(Vr_d, Vr_s)$, $(Vr_d, F_p)$, $(Vr_d, Vz_p)$, $(Vr_d, A_p)$, $(Vr_d, Vr_p)$, $(Vr_d, S_d)$, $(Vr_d, F_d)$, $(Vr_d, Vr_d)\}$.

Поскольку такие элементы полученного произведения, как $(F_s, F_p)$ и $(F_p, F_s)$ будут в конечном итоге иметь одни и те же угрозы, можно считать подобные элементы равными. Обозначим множество возможных переходов в полученной ранее общей схеме информационных процессов как $P$. Множество $P$ будет являться частью декартового произведения множеств $Q$ и $W$:

$P \subset (Q \times W) = \{(F_s, F_p), (F_s, Vz_p), (F_s, A_p), (F_s, Vr_p), (Vr_s, Vr_p), (F_p, F_p), (F_p, F_d), (Vz_p, Vz_p), (Vz_p, Vr_p), (Vz_p, S_d), (A_p, A_p), (A_p, Vr_p), (A_p, S_d), (Vr_p, S_d), (Vr_p, Vr_d)\}$.

Для удобства обозначим каждый переход $P_i$, $i$ от 1 до 15.

$(F_s, F_p) = P_1$, $(F_s, Vz_p) = P_2$, $(F_s, A_p) = P_3$, $(F_s, Vr_p) = P_4$, $(Vr_s, Vr_p) = P_5$, $(F_p, F_p) = P_6$, $(F_p, F_d) = P_7$, $(Vz_p, Vz_p) = P_8$, $(Vz_p, Vr_p) = P_9$, $(Vz_p, S_d) = P_{10}$, $(A_p, A_p) = P_{11}$, $(A_p, Vr_p) = P_{12}$, $(A_p, S_d) = P_{13}$, $(Vr_p, S_d) = P_{14}$, $(Vr_p, Vr_d) = P_{15}$.

$P = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}\}$.

Множество типов угроз (множество $T$ является семейством множеств, так как включает элементы, которые являются множествами): $T = \{K, C, A\}$, где $K$ – угрозы конфиденциальности; $C$ – угрозы целостности; $A$ – угрозы доступности. Множество классов угроз конфиденциальности: $K = \{K_1, K_2, K_3, K_4\}$. Множество классов угроз целостности: $C = \{C_1, C_2, C_3, C_4\}$. Множество классов угроз доступности: $A = \{A_1, A_2, A_3, A_4\}$. Для получения угрозы необходимо произвести декартово перемножение множеств $P$ и $T$. Обозначим множество угроз – $U$: $U \subset (P \times T)$.

В качестве примера далее приведены угрозы для перехода $P_9$ (рис. 7). Обработка, виртуальная среда ($Vr_p$) – обработка, визуальная среда ($Vz_p$).

Объекты, участвующие в описании перехода: виртуальное адресное пространство процесса (обработка, виртуальная среда); бумажный носитель, человек (обработка, визуальная среда); преобразователь 1 – устройства вывода (монитор, принтер); преобразователь 2 – устройства ввода (клавиатура, мышь, сканер, цифровая камера).

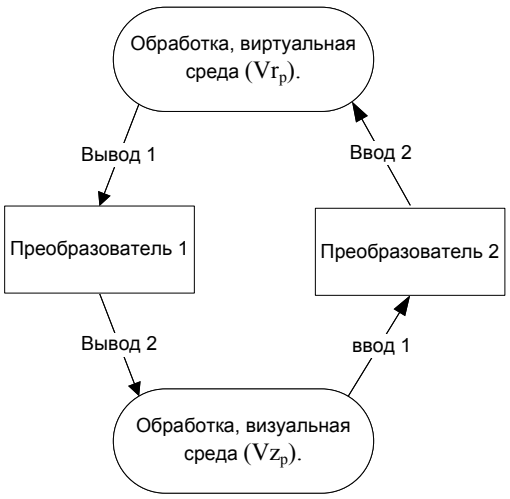


Рис. 7. Переход «Обработка, виртуальная среда – обработка, визуальная среда»

Угрозы конфиденциальности: 1) подмена информации в виртуальном адресном пространстве процесса; 2) получение информации злоумышленником; 3) вывод информации на несанкционированный преобразователь (монитор, принтер), съем побочных излучений с преобразователя; 4) вывод информации за пределы санкционированной зоны.

Угрозы целостности: 1) получение информации из виртуального адресного пространства несанкционированного процесса; 2) ввод информации злоумышленником; 3) получение информации с несанкционированного преобразователя (например, клавиатуры); 4) помехи, ошибки.

Угрозы доступности: 1) недоступность виртуального адресного пространства; 2) отсутствие доступа к ЭВМ у санкционированного пользователя; 3) недоступность преобразователя; 4) недоступность канала.

В ходе работы была построена типовая схема информационных процессов и ее частные случаи – схема информационных процессов с физическим доступом, схема информационных процессов с использованием средств автоматизации и схема информационных процессов без использования средств автоматизации. Подготовлена общая схема информационных процессов, которая включает в себя 9 состояний в различных средах и 15 переходов между этими состояниями. Общая схема является основой в разработанной модели угроз. Выделены типовые угрозы: конфиденциальности, целостности и доступности. Суммарно получено 12 классов угроз, возникающих при работе с информацией. Таким образом, сформирован новый подход к построению модели угроз защищаемой информации.

Работа выполнена в рамках проекта 7.701.2011 (проект 1/12) при поддержке Министерства образования и науки Российской Федерации.

*Литература*

1. Принципы моделирования механизмов воздействия вредоносных программы на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.С. Александров, Г.И. Рябин и др. // Доклады ТУСУРа. – 2008. – № 2(18). – С. 135–136.

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК. – Введ. 2008-15-02.

---

**Конев Антон Александрович**
Канд. техн. наук, доцент каф. комплексной информационной безопасности
электронно-вычислительных систем ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: kaa1@kibevs.tusur.ru

Konev A.A.

**Approach to creation protected information model**

Approach to creation model, based on the use of information processes schemes, is suggested. Information processes are constructed taking into account actions with protected information and its distribution environments. This takes into account conversion of the information presentation in passing from one medium to another.

**Keywords:** information security, threat model, information process.

---