Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Воробьев Антон Александрович
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Факультет компьютерных технологий, каф. ИБАС
Аспирант каф. ИБАС
Vorobev Anton Alexandrovich
«Komsomolsk-on-Amur state technical University», faculty of computer technologies
Post-graduate student of Department of information security of automated systems
E-Mail: zeromem@mail.ru

Моделирование и оценка системы защиты конфиденциальной информации для высших учебных заведений

Modeling and assessment security system of confidential information for colleges

Аннотация: В данной статье рассматриваются вопросы, связанные с обеспечением информационной безопасности предприятий на примере высшего учебного заведения. Рассматривается математическая модель для анализа возможности утечки конфиденциальной информации для предприятий на примере ВУЗа.

Abstract: In this article the questions connected with ensuring information security of the enterprises on the example of a higher educational institution are considered. The mathematical model for the analysis of possibility of confidential information distribution for the enterprises is considered.

Ключевые слова: защита информации; конфиденциальная информация; моделирование; безопасность данных; информационная система.

Keywords: information security; confidential information; modeling; data security; information system.

***

Введение

В работе [1] предложена схема организации *информационной системы (ИС)* и *локальной вычислительной сети (ЛВС)* предприятия для минимизации возможности утечки *конфиденциальной информации (КИ)* за счет *преднамеренного несанкционированного доступа (ПНСД),* и атак из *глобальных сетей обмена информацией (ГСОИ).* В данной статье рассматриваются вопросы моделирования атак злоумышленников на информационные системы предприятий, где циркулирует КИ, количественной оценки возможности атак.

Математическая модель ИС предприятия

В качестве модели ИС мы предлагаем использовать ориентированный, взвешенный, раскрашенный мультиграф:

$IS = (A, V, dom, cod, col, typ, v_0)$, где

A – множество ребер, V – множество вершин, $v_0 \in V$ – выделенная вершина для базы данных в информационной системе из нее не выходит ни одной стрелки, вообще говоря, таких вершин может быть несколько в этом случае они образуют множество V_{db} дополняющее модель, $dom: A \to V$, $cod: A \to V$ – функции задающие для каждого ребра начало и конец соответственно, $col: V \to \{0,1,2,3,4,5\}$, функция задающая раскраску вершин графа в

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

соответствии с классификацией предложенной в [1], вершина раскрашивается цветом *0*, если это программно-аппаратное средство обеспечения информационной безопасности (сервер доступа, межсетевой экран, комплекс шифрования), $typ: A \to [0,1]$ – функция раскраски стрелок принимающая для некоторого ребра значение *0*, если данное ребро соответствует реализации угрозы внутренним нарушителем и *1*, если внешним. Под внутренним нарушителем будем понимать сотрудника предприятия или лицо, имеющее непосредственный доступ к ЛВС предприятия, а под внешним злоумышленника пытающегося получить ПНСД из ГОСИ. В дальнейшем мы не будем рассматривать атаки внутренних нарушителей на автоматизированные рабочие места расположенные вовне пределов информационной системы.

Ориентация ребер графа *IS* задает направление движения злоумышленника по информационной системе.

Ясно, что при использовании данной модели автономным рабочим местам на предприятии не имеющих подключения к ГОСИ и ЛВС предприятия будут соответствовать компоненты связности графа *IS* и данные вершины следует считать наиболее защищенными, пусть они образуют множество V_{avt}, более формально

$V_{avt} \subseteq V$,

$\forall v \in V_{avt}, \neg\exists a \in A | dom(a) = v$,

$\neg\exists a` \in A | cod(a`) = v$.

$\forall v \in V_{avt}$, $col(v) = 4$.

$\neg\exists a` \in A | dom(a`) = v_0$.

Опишем дополнительные свойства графа *IS*:

$\forall v \in V$,

$col(v)=5 \Rightarrow \neg\exists a \in A | cod(a) = v$,

$\exists! a` \in A | dom(a`) = v$,

$col(cod(dom(a`))) = 0$,

$typ(a`) = 1$, т.е. для всех вершин которым соответствуют узлы расположенные вовне ИС, существует единственное ребро с началом в этой вершине и концом в вершине соответствующей некоторому программно-аппаратному средству обеспечивающему функции сервера доступа, причем данное ребро соответствует атаке реализуемой из ГОСИ, пусть они образуют множество A_{in}, а вершину соответствующую серверу доступа обозначим Z. Пусть

$\forall a \in A$ $cod(a) = v_0$ образуют множество A_{db}, причем $\forall a \in A_{db}$ $col(dom(a)) = 0$, тогда

$\forall a \in A$, $dom(a) = u$,

$cod(a) = v$,

$typ(a) = 0 \Rightarrow \exists a` \in A$,

$dom(a`) = u$, $cod(a`) = v$,

$typ(a`) = 1$, т.е. если есть возможность у внутреннего нарушителя из узла *u*, реализовав некоторую угрозу и перейти в узел *v*, то обязательно существует возможность перейти из *u* в *v* и у внешнего нарушителя.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

$\forall a \in A \backslash (A_{db} \cup A_{in})$,

$dom(a) = u$,

$cod(a) = v$,

$\exists a` \in A, dom(a`) = v$,

$cod(a`) = u$, т.е. для всех стрелок из u в v существует обратная за исключением выходящих из вершин цвета 5 и входящих в v_0.

Еще одним важным свойством является то, что

$\neg \exists a` \in A \mid col(dom(a)) \neq 0$,

$col(cod(a)) \neq 0 \Rightarrow col(dom(a)) \neq col(cod(a))$, т.е. не существует ребер инцидентных вершинам раскрашенным в одинаковый цвет, за исключением вершин цвета 0. Более того

$\forall a \in A \mid dom(a) = u$,

$cod(a) = v$,

$col(u) = 0 \Rightarrow col(v) \neq 0$,

$col(u) \neq 0 \Rightarrow col(v) = 0$, т.е. для всякого ребра либо его начало либо конец окрашены в цвет 0.

Операции для предложенной модели

Для предложенной математической модели введем две операции – удаления вершины и добавления вершины.

Пусть $IS_1 = (A, V, dom, cod, col, typ, v_0)$, удаление вершины из графа у IS_1 осуществляется в соответствии со следующими правилами (удалить вершину v_0 можно тогда и только тогда, когда $\neg \exists v` \in V \mid v` \neq v_0$, т.е. вершина v_0 - единственная):

$IS_1 \backslash \{v\} = IS_2$,

$IS_2 = (A`, V`, dom`, cod`, col`, typ`, v`_0)$, удовлетворяющая следующим условиям:

Пусть

$Dom(v) = \{ a \in A \mid dom(a) = v\}$,

$Cod(v) = \{ a \in A \mid cod(a) = v\}$,

$DDom(v) = \{(a,v) \mid a \in Dom(v)\}$,

$CCod(v) = \{(a,v) \mid a \in Cod(v)\}$,

$Typ = \{(a,typ(v)) \mid a \in Cod(v) \cup (Dom(v)\}$.

При удалении вершины $v \in V$ следует строго придерживаться следующих правил:

$col(v) \neq 0 \Rightarrow$

$A` = A \backslash (Dom(v) \cup Cod(v))$,

$V` = V \backslash v$,

$dom` = dom \backslash DDom(v)$,

$cod` = cod \backslash CCod(v)$,

$col` = col \backslash \{(v,col(v))\}$,

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

$typ` = typ\backslash Typ,$

$v`_0 = v_0.$

$col(v) = 0 \Rightarrow$

$A` = A\backslash(Dom(v) \cup Cod(v)),$

$V` = V\backslash v,$

$dom` = dom\backslash DDom(v),$

$cod` = cod\backslash CCod(v),$

$col` = col\backslash\{(v,col(v))\},$

$\neg\exists v` \in V` \mid col(v`) \neq 4,$

$dom`(v`) = \varnothing, cod`(v`) = \varnothing,$

$typ` = typ\backslash Typ, v`_0 = v_0.$

Определим операцию добавления вершины к модели. Пусть $IS_1 = (A, V, dom, cod, ver, col, typ, v_0)$, добавление вершины v^* в графа IS_1 осуществляется в соответствии со следующим правилом:

$IS_1 \cup \{v^*\} = IS_2,$

$IS_2 = (A`, V`, dom`, cod`, col`, typ`, v`_0).$

Далее опишем алгоритм добавления вершины в зависимости от цвета в который она окрашена:

$col(v^*)=4 \Rightarrow IS_2 = (A, V \cup \{v^*\}, dom, cod, col \cup \{(v^*,4)\}, typ, v_0).$

$col(v^*)=1 \Rightarrow$ добавление вершины производится с добавлением четырех ребер соответствующих атакам внутреннего нарушителя расположенного в добавляемой вершине, атаке внутреннего нарушителя расположенного внутри информационной системы на эту вершину, атаке внешнего нарушителя на данный узел и атаке из данной вершины вовне, причем один из концов добавляемых ребер должен быть вершиной с цветом 0, если это сделать невозможно, то и добавить вершину с данными свойствами нельзя.

$IS_2 = (A`, V \cup \{v^*\}, dom`, cod`, col \cup \{(v^*,1)\}, typ`, v_0),$ где

$A` = A \cup \{a_1, a_2, a_3, a_4\},$

$\exists v` \in V \mid col(v`) = 0,$

$dom`(a_1) = v^*, dom`(a_4) = v^*, dom`(a_2) = v`, dom`(a_3) = v`,$

$cod`(a_1) = v`, cod`(a_4) = v`, cod`(a_2) = v^*, cod`(a_3) = v^*,$

$typ`(a_1) = 0, typ`(a_4) = 1, typ`(a_2) = 0, typ`(a_3) = 1.$

Вершины цвета *2* добавляются аналогично вершинам цвета *1*.

$col(v^*)=5 \Rightarrow$ добавление вершины производится с добавлением одного ребра один конец которого это вновь добавляемая вершина, а второй это Z.

$IS_2 = (A`, V \cup \{v^*\}, dom`, cod`, col \cup \{(v^*,4)\}, typ`, v_0),$ причем

$A` = A \cup \{a_1\},$

$dom`(a_1) = v^*,$

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

$cod`(a_1) = Z$,

$typ`(a_1) = 1$.

$col(v^*)=3 \Rightarrow$ добавление вершины производится с добавлением восьми ребер соответствующих атакам внутреннего нарушителя расположенного в добавляемой вершине, атаке внутреннего нарушителя расположенного внутри информационной системы на эту вершину, атаке внешнего нарушителя на данный узел и атаке из данной вершины вовне, причем один из концов добавляемых ребер должен быть вершиной с цветом 0, четыре ребра для одной вершины окрашенной цветом 0 и 4 ребра для другой, если это сделать невозможно, то и добавить вершину с данными свойствами нельзя.

$IS_2 = (A`, V \cup \{v^*\}, dom`, cod`, col \cup \{(v^*,3)\}, typ`, v_0)$, где

$A` = A \cup \{a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8\}$,

$\exists v`, v`` \in V | \ col(v`) = 0, col(v``) = 0, v` \neq v``$.

$dom`(a_1) = v^*, dom`(a_4) = v^*, dom`(a_2) = v`, dom`(a_3) = v`,$

$cod`(a_1) = v`, cod`(a_4) = v`, cod`(a_2) = v^*, cod`(a_3) = v^*,$

$typ`(a_1) = 0, typ`(a_4) = 1, typ`(a_2) = 0, typ`(a_3) = 1$.

$dom`(a_5) = v^*, dom`(a_8) = v^*, dom`(a_6) = v`, dom`(a_7) = v`,$

$cod`(a_5) = v`, cod`(a_8) = v`, cod`(a_6) = v^*, cod`(a_7) = v^*,$

$typ`(a_5) = 0, typ`(a_8) = 1, typ`(a_6) = 0, typ`(a_7) = 1$.

$col(v^*)=0 \Rightarrow$ добавление вершины производится с добавлением четырех ребер соответствующих атакам внутреннего нарушителя расположенного в добавляемой вершине, атаке внутреннего нарушителя расположенного внутри информационной системы на эту вершину, атаке внешнего нарушителя на данный узел и атаке из данной вершины вовне, причем один из концов добавляемых ребер должен быть вершиной с цветом 0, если это сделать невозможно, то и добавить вершину с данными свойствами нельзя.

$IS_2 = (A`, V \cup \{v^*\}, dom`, cod`, col \cup \{(v^*,0)\}, typ`, v_0)$, где

$A` = A \cup \{a_1,a_2,a_3,a_4\}$,

$\exists v` \in V | \ col(v`) = 0$,

$dom`(a_1) = v^*, dom`(a_4) = v^*, dom`(a_2) = v`, dom`(a_3) = v`,$

$cod`(a_1) = v`, cod`(a_4) = v`, cod`(a_2) = v^*, cod`(a_3) = v^*,$

$typ`(a_1) = 0, typ`(a_4) = 1, typ`(a_2) = 0, typ`(a_3) = 1$.

Для добавления вершин соответствующих дополнительным вершинам базы данных предприятия необходимо дополнить множество Vdb дополнительным элементом, добавить новую вершину цвета 0 без исходящих ребер к модели и связать с ней вновь добавленную вершину для базы данных без исходящих ребер. То есть необходимо выполнить два шага:

1. $IS_2 = (A`, V \cup \{v^*\}, dom`, cod`, col \cup \{(v^*,0)\}, typ`, v_0)$, где

$A` = A \cup \{a_1,a_2 \}$,

$\exists v` \in V | \ col(v`) = 0$,

$dom`(a_1) = v`, dom`(a_2) = v`,$

$cod`(a_1) = v^*, cod`(a_2) = v^*,$

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

$typ`(a_1) = 0, typ`(a_2) = 1.$

2. $IS_3 = (A`, V \cup \{v`\}, dom`, cod`, col \cup \{(v^*,0)\}, typ`, V_{db}=V_{db} \cup v_0 \cup \{v`\})$, где

$A` = A \cup \{a_1,a_2\},$

$dom`(a_1) = v^*, dom`(a_2) = v^*,$

$cod`(a_1) = v`, cod`(a_2) = v`,$

$typ`(a_1) = 0, typ`(a_2) = 1.$

Введенные операции позволяют выполнять преобразование, получая новые модели из уже существующих.

Практическое применение

Для примера преобразуем модель, приведенную на рис. 1 к типовой модели малого предприятия состоящего из директора, отдела кадров, бухгалтерии и одного отдела занимающегося оформлением документов с контрагентами, причем у предприятия есть выход в сеть Интернет, отсутствуют выделенные автоматизированные места с подключением к ГОСИ, есть база данных конфиденциальной информации. Последовательность преобразования приведена на рис. 2-3.

Схеме ЛВС предприятия со структурой применяемых средств защиты информации приведенной в [1] соответствует граф рис. 1.

На рисунке 2 представлен граф после удаления всех вершин цвета 4 и цвета 2.

На рисунке 3 представлен граф после удаления всех вершин цвета 1 расположенных слева.

При помощи предложенной модели можно описать достаточно большой класс ЛВС предприятий, причем при правильной конфигурации программно-аппаратный средств защиты информации на рабочих местах, настройке антивирусной защиты и средств защиты от НСД возможно удовлетворить всем требованиям НМД.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

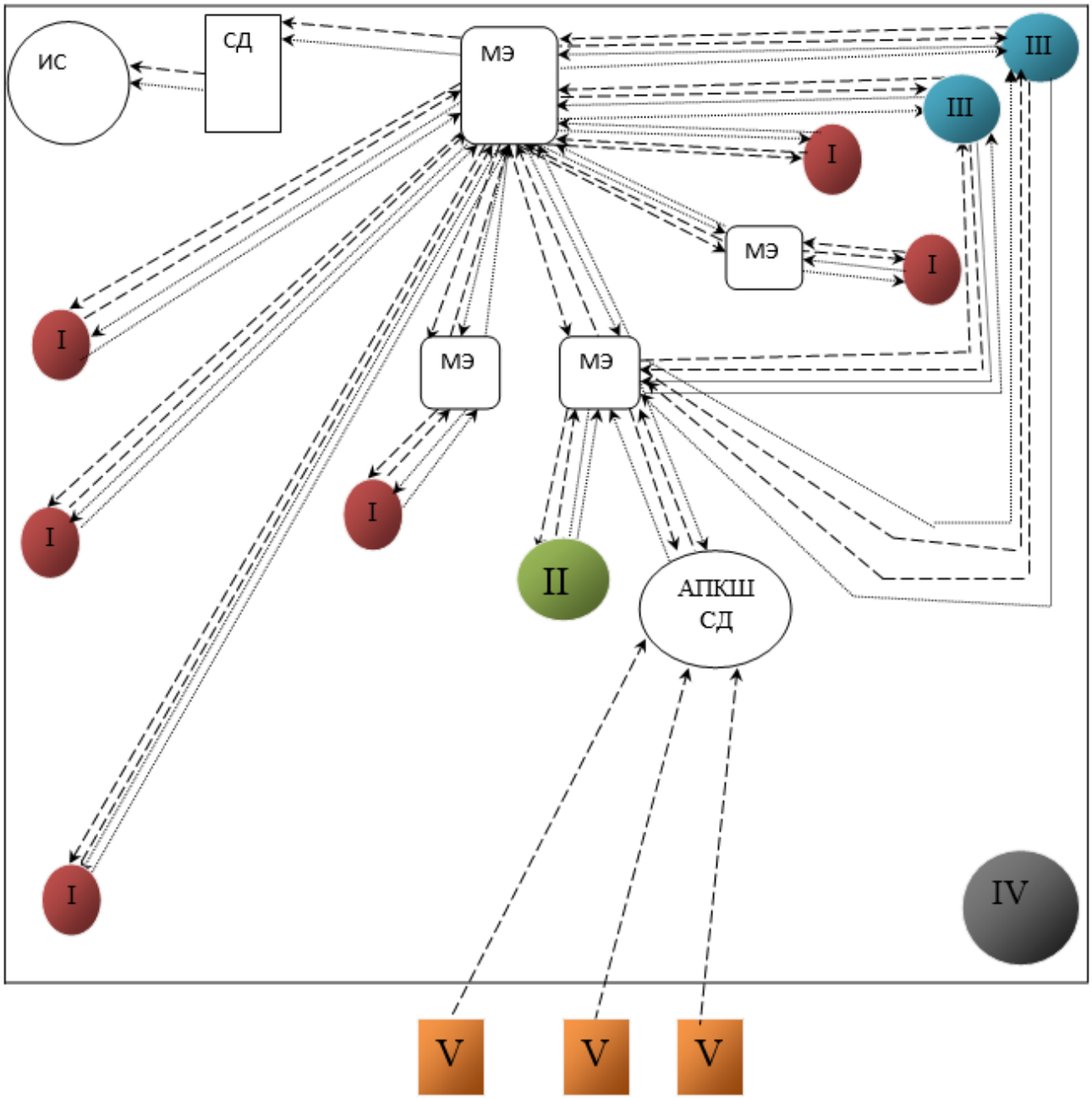

Рис. 1. *Граф схемы локальной вычислительной сети предприятия*

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

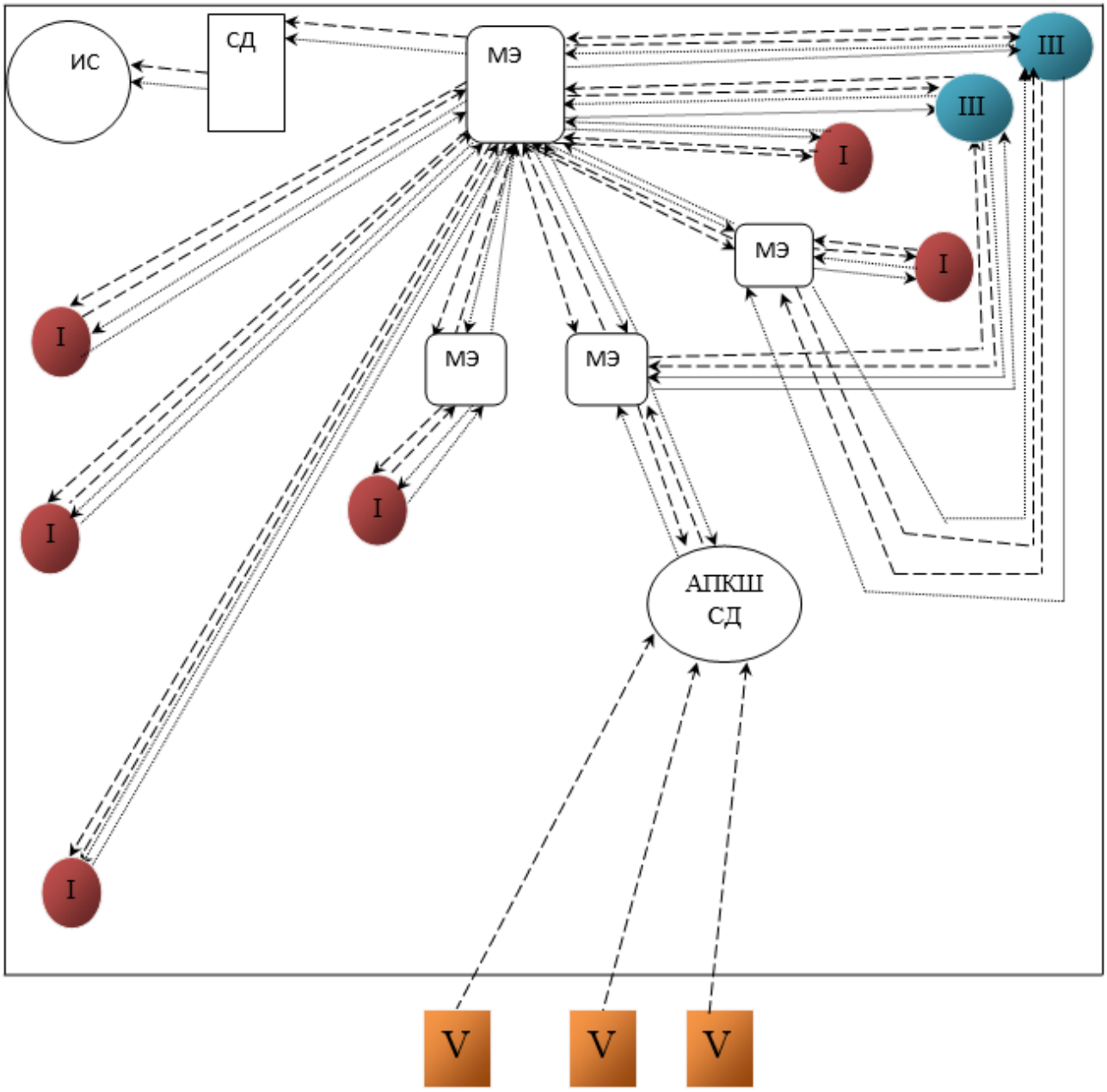

Рис. 2. *Измененный граф схемы локальной вычислительной сети предприятия*

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

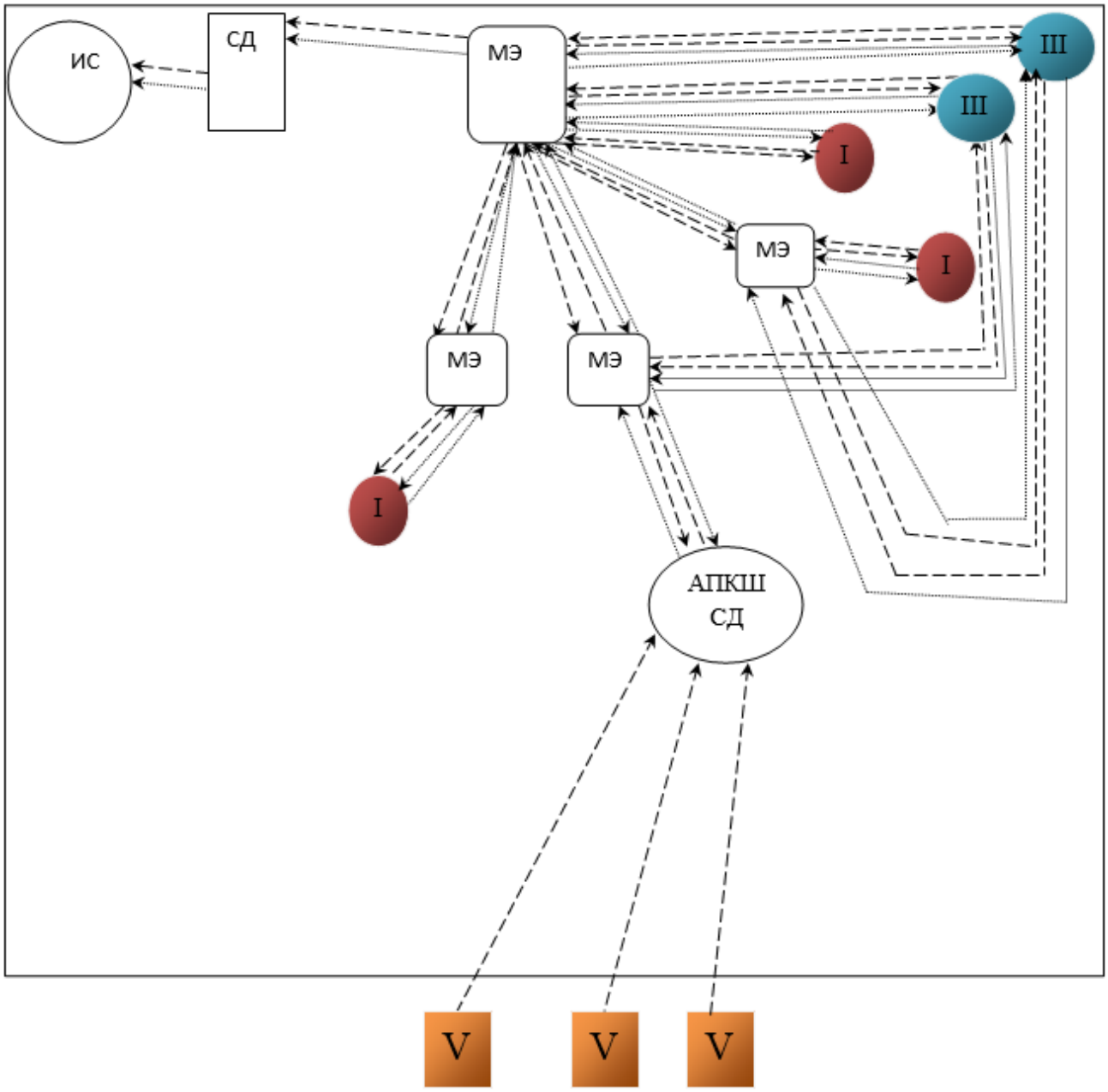

Рис. 3. *Окончательный вариант графа схемы локальной вычислительной сети предприятия*

Заключение

В работе предложена математическая модель взвешенного, ориентированного, раскрашенного мультиграфа для моделирования и оценки вероятности реализации угроз внутренних и внешних нарушителей. Введены операции позволяющие, для заданных мультиграфов, получить новые, путем добавления и удаления вершин мультиграфа, без нарушения связности. Дальнейшие исследования предполагают введение специализированных операций для объединения и пересечения мультиграфов соответствующих различным ИС, задание алгебры и категории над мультиграфами *IS*.

Отдельный интерес представляет рассмотрение дополнения модели функциями для применения аппарата математической статистики и теории вероятностей.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

ЛИТЕРАТУРА

1. Трещев И.А., Григорьев Я.Ю., Воробьев А.А. Система защиты конфиденциальной информации для высших учебных заведений «Электронный университет» //Интернет-журнал «Науковедение». 2013 №1 (14) [Электронный ресурс].-М. 2013. – Режим доступа: http://naukovedenie.ru/PDF/44tvn113.pdf, свободный – Загл. с экрана.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. Гриф Министерства образования и науки. – М.: Горячая линия-Телеком, 2006. – 544 с.: ил. ISBN 5-93517-292-5.

3. Воробьев А.А. Алгебраические методы исследования таксономий уязвимостей вычислительных сетей и компьютерных систем/ Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С 12-15.

4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов. Под ред. Зайцева А.П. и Шелупанова А.А. Гриф министерства образования и науки РФ. – 7-е изд., испр. и доп.- М.: Горячая линия - Телеком, 2012.- 425 с.: ил. ISBN 978-5-9912-0084-4 .

5. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем: Монография. – Томск: Изд-во В-Спектр, 2007.- 278 с.: ил.

6. Трещев И.А. Оценка временных затрат для осуществления распределенного перебора в гетерогенных системах при помощи временных волновых систем //Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С. 141-148.

Рецензент: Д.т.н., помощник ректора по информатизации ФГБОУ ВПО «Комсомольский-на-Амуре Государственный технический университет» С.В. Биленко.