На правах рукописи

Новохрестов Алексей Константинович

МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ АТРИБУТИВНЫХ МЕТАГРАФОВ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Томск 2018

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Научный руководитель –	Шелупанов Александр Александрович, доктор технических наук, профессор
Официальные оппоненты:	Новиков Сергей Николаевич, доктор технических наук, доцент, заведующий кафедрой безопасности и управления в телекоммуникациях Сибирского государственного университета телекоммуникаций и информатики
	Ложников Павел Сергеевич, кандидат технических наук, доцент, заведующий кафедрой «Комплексная защита информации» Омского государственного технического университета
Ведущая организация –	Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский государственный авиационный технический университет»

Защита состоится «28» декабря 2018 г. в 10:00 часов на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г. Томск, пр. Ленина 40, ауд. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУР по адресу: 634045, г. Томск, ул. Красноармейская 146, а также на сайте ТУСУР: https://postgraduate.tusur.ru/urls/3p71shui

Автореферат разослан «___» _____ 2018 г.

Ученый секретарь
диссертационного совета  Зыков Дмитрий Дмитриевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Проблема обеспечения безопасности компьютерных сетей не теряет актуальности с момента их появления и широкого распространения до наших дней. Так, согласно исследованию компании Positive Technologies, к концу 2017 года сложность преодоления защищенного сетевого периметра в 56% случаев оценивалась как тривиальная. Вместе с этим, технологии постоянно развиваются: появляются новые виды угроз, и обеспечение безопасности компьютерных сетей эволюционирует в обеспечение безопасности системы «Интернет вещей».

Неотъемлемым этапом процесса обеспечения безопасности является определение перечня актуальных угроз. Однако до определения актуальности необходимо составить как можно более обширный перечень угроз, т.е. осуществить идентификацию угроз.

При этом вопросы обеспечения сетевой безопасности актуальны как для крупных компаний, так и для небольших организаций. При этом очевидно, что ресурсы, которые могут быть выделены на обеспечение безопасности, будут отличаться. Это влияет не только на возможные затраты на техническое оснащение, но и на квалификацию специалистов, которых организация может нанять.

Профессиональный уровень, а также субъективное мнение эксперта при использовании существующих подходов к построению перечней угроз информационных систем существенно влияет на итоговый результат.

Актуальной является задача по разработке эффективной методики составления перечня угроз информационной безопасности компьютерных сетей, при использовании которой будет минимизировано влияние профессионального уровня и субъективного мнения эксперта.

Целью исследования является повышение объективности составления перечня угроз информационной безопасности компьютерных сетей.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. выполнить анализ текущего состояния предметной области: использующихся при составлении перечней угроз моделей компьютерных сетей и подходов к построению моделей угроз;
2. разработать модель компьютерной сети, позволяющую описать структуру системы на достаточном для составления перечня угроз уровне детализации;
3. разработать модель угроз компьютерной сети, учитывающую максимально возможное количество угроз;
4. разработать методику составления перечня угроз информационной безопасности компьютерных сетей;
5. апробировать методику и модели на практике.

Объектом исследования данной работы является информационная безопасность компьютерных сетей в условиях существования угроз системе и обрабатываемой в ней информации.

Под рассматриваемыми компьютерными сетями подразумеваются локальные вычислительные сети (ЛВС), представляющие собой систему, обеспечивающую обмен данными между подсетями, узлами сети и установленным на них программным обеспечением.

Предметом исследования является модель угроз информационной безопасности компьютерных сетей.

Основные **методы исследования**, примененные в диссертационной работе – это методы моделирования, системного анализа, теории графов и теории защиты информации.

Научная новизна результатов работы и проведенных исследований заключается в следующем:

1. Предложена модель компьютерной сети, основанная на атрибутивных метаграфах, отличающаяся наличием связей между различными уровнями программного обеспечения компьютерных систем.
2. Предложена модель угроз информационной безопасности компьютерных сетей, отличающаяся формированием типов угроз на основе элементарных операций над метаграфами.
3. Разработана новая методика составления перечня угроз информационной безопасности компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами.

Теоретическая значимость результатов исследования заключается в том, что:

1. Применительно к разработке модели угроз информационной безопасности компьютерной сети результативно использован математический аппарат теории графов для моделирования компьютерных сетей.
2. Изучена связь между типами угроз и базовыми операциями над метаграфами.

Практическая значимость результатов исследования состоит в следующем:

1. Представлены методические рекомендации по формированию перечня угроз, направленных на нарушение конфиденциальности и целостности информационной системы.
2. Разработана и внедрена методика составления перечня угроз информационной безопасности, использующая разработанные модели компьютерной сети и угроз. Внедрение методики позволило при применении к разрабатываемой системе коммерческого учета энергоресурсов обнаружить на 18% больше угроз, чем ранее было обнаружено экспертами.

Положения, выносимые на защиту:

1. Модель компьютерной сети, основанная на атрибутивных метаграфах, позволяет описать компоненты программного обеспечения компьютерных сетей (прикладное, системное и сетевое программное обеспечение) и все возможные связи между ними (сетевые протоколы, драйверы, и т.п.) для построения модели угроз.

Соответствует пункту 3 паспорта специальности: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

2. Модель угроз информационной безопасности компьютерных сетей позволяет описать угрозы более полно относительно существующих решений: в банке данных угроз ФСТЭК России представлено 25 из 36 типов угроз безопасности информационной системы, выделенных в данной работе.

Соответствует пункту 3 паспорта специальности: методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

3. Методика составления перечня угроз информационной безопасности компьютерных сетей позволила увеличить на 18% количество учтенных угроз при разработке автоматизированной системы коммерческого учета энергоресурсов.

Соответствует пункту 15 паспорта специальности: модели и методы управления информационной безопасностью.

Обоснованность и достоверность результатов работы подтверждается их внутренней непротиворечивостью и положительным эффектом от внедрения научных исследований в работу действующего предприятия, о чем свидетельствует соответствующий Акт о внедрении. Использовано сравнение авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Внедрение результатов. Результаты диссертационной работы внедрены в деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов, а также в учебный процесс Томского государственного университета систем управления и радиоэлектроники.

Личный вклад. В работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных работ написана в соавторстве с сотрудниками научной группы. Постановка задачи исследования осуществлялась научным руководителем д.т.н., профессором Шелупановым А.А.

Апробация работы. Основные и промежуточные результаты исследования докладывались и обсуждались на следующих конференциях:

— VI Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных: Проблемы и пути их решения» (Брянск, 2014);

— Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР» (Томск, 2014, 2015, 2016);

— Российской научно-технической конференции «Инновации и научно-техническое творчество молодежи» (Новосибирск, 2014);

— XV Всероссийской научно-практической конференции «Проблемы информационной безопасности государства, общества, личности» (Иркутск, 2014);

— XI Международной научно-технической конференции «Динамика систем, механизмов и машин» (Омск, 2014);

— XI Международной научно-практической конференции «Электронные средства и системы управления» (Томск, 2015, 2016, 2017);

— XIII Международной конференции студентов, аспирантов и молодых ученых «Перспективы развития фундаментальных наук» (Томск, 2016);

— V всероссийской научно-технической конференции «Студенческая наука для развития информационного общества» (Ставрополь, 2016);

— Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности» (Самара, 2017);

Докладывались и обсуждались на заседаниях кафедры Комплексной информационной безопасности электронно-вычислительных систем ТУСУР и IEEE семинарах «Интеллектуальные системы моделирования, проектирования и управления» в г. Томске.

Результаты настоящей работы использовались в реализации комплексного проекта по созданию высокотехнологичного производства интеллектуальных приборов энергоучета, разработанных и изготовленных на базе отечественных микроэлектронных компонентов, и гетерогенной автоматизированной системы мониторинга потребляемых энергоресурсов на их основе (контракт № 02.G25.31.0107 от 14 августа 2014 г).

Работа выполнена при поддержке Министерства образования и науки РФ в соответствии с государственным заданием ТУСУР на 2017–2019 гг. Проект № 2.8172.2017/8.9 «Метод и модели определения уровня защищенности информационных систем».

Публикации по теме диссертации. По материалам исследования опубликовано 16 работ, в том числе 2 работы в изданиях, рекомендованных ВАК РФ.

Структура и объем работы. Диссертация содержит введение, три главы, заключение, 1 приложение и список источников из 108 наименований. Объем диссертационной работы: 114 страниц, в том числе 14 таблиц и 14 рисунков.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулирована цель, определены задачи, научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе рассматриваются подходы к построению моделей компьютерных сетей, применяемые при идентификации угроз и оценке

защищенности, а также непосредственно подходы к описанию и идентификации угроз и построению моделей угроз компьютерных сетей и информационных систем.

В результате проведенного анализа подходов к построению моделей компьютерных сетей можно заключить, что с их помощью невозможно подробно описать, чем являются объекты в информационной системе (т.е. описать их параметры), а также способы их взаимодействия между собой. Для того, чтобы наиболее полно описать угрозы информационной безопасности компьютерной сети, используемая для этого модель самой компьютерной сети должна удовлетворять следующим требованиям:

1) необходимо учитывать иерархичность программного обеспечения компьютерных сетей;

2) необходимо учитывать возможность существования нескольких связей между двумя элементами;

3) необходимо учитывать, что элементы и связи между ними имеют параметры.

В ходе анализа подходов к построению моделей угроз информационной безопасности информационных систем и, в частности, компьютерных сетей, были выявлены следующие недостатки:

1) в моделях угроз присутствуют элементы модели нарушителя, либо модель нарушителя оказывает непосредственное влияние на формирование перечня угроз;

2) отсутствие системности – в рамках одной модели описываются как обобщенные угрозы, так и частные случаи;

3) отсутствует разделение на угрозы, направленные на систему и информацию;

4) построение перечней угроз основывается на субъективном мнении эксперта.

Ключевой недостаток всех моделей заключается в том, что ни в одной из них нет описания угроз информационной системе в явном виде. Все внимание уделяется угрозам информации, обрабатываемой в рассматриваемой информационной системе, например в информационной системе персональных данных.

Каждая из рассмотренных моделей может учитывать те или иные угрозы, которые не описаны в другой.

Также во многих рассмотренных моделях нет математической формализации, т.е. угрозы представлены посредством словесных описаний, а последовательность идентификации угроз рассматриваемой системе общими указаниями, без пошагового описания действий. Это часто приводит к тому, что эксперты могут трактовать одну и ту же методику по-разному, более того эксперты, зачастую, не имеют прямого отношения к организации, что вносит дополнительные неточности в формирование модели угроз. К данному пункту также можно отнести отсутствие в подходах к формированию перечней угроз

обоснования классификации угроз и, как следствие, обоснования полноты предлагаемой классификации.

Во второй главе предлагается модель компьютерной сети и модель угроз информационной безопасности компьютерной сети в совокупности с подходом к классификации угроз, а также описывается методика определения перечня угроз, использующая разработанные модели.

Модель компьютерной сети на основе атрибутивных метаграфов позволяет описывать компоненты программного обеспечения компьютерных сетей и все возможные связи между ними. В работе рассматривается только программные элементы компьютерных сетей (компоненты программного обеспечения (ПО) компьютерных сетей) и связи между ними. К компонентам программного обеспечения в данном случае относится прикладное, системное и сетевое программное обеспечение. Связи подразумеваются не только между элементами, находящимися на одном уровне, но и обозначающие вложенность одних элементов в другие. Т.е. прикладное ПО функционирует в рамках операционных систем (ОС), которые представляют системное ПО. В свою очередь операционные системы функционируют в рамках локальных вычислительных сетей (или подсетей), реализующихся посредством сетевого ПО. Таким образом выделяется три уровня программного обеспечения компьютерных сетей, для удобства уровни обозначены как уровень ПО, уровень ОС, уровень ЛВС.

В качестве математического аппарата для реализации модели были выбраны атрибутивные метаграфы. Метаграф содержит и согласует между собой два основных свойства системы: единство (совокупность взаимосвязанных элементов) и делимость (каждый элемент системы – тоже система). В связи с этим из системы можно выделить подсистемы, что позволяет в определенной ситуации сосредоточить внимание на системе или ее подсистеме.

Атрибутивный метаграф вложенности n представляется как упорядоченная пара:

$$G = (X, E),$$

где G – метаграф вложенности n;

$X = \{x_i\}, i = \overline{1,n}$ – непустое конечное множество вершин;

$E = \{e_k\}, k = \overline{1,m}$ – непустое конечное множество ребер.

Каждое ребро n-мерного графа соединяет два подмножества множества вершин:

$$e_k = (V_i, W_i),$$

где $V_i, W_i \subseteq X$;

$V_i \cup W_i \neq \emptyset$;

i – уровень вложенности.

Также существуют функции, обозначающие вложенность вершин и ребер метаграфа:

$$f_1^l: g_1^l(x_1^l, e_1^l) \to x_2^p, f_2^p: g_2^p(x_2^p, e_2^p) \to x_3^m, \dots, f_{n-1}^t: g_{n-1}^t(x_{n-1}^t, e_{n-1}^t) \to x_n,$$

где $l, p, r, \dots, t$ – номер вершин и ребер на соответствующем уровне.

Вершины и ребра атрибутивного метаграфа характеризуются множеством атрибутов:

$$x_i = \{atr_j\},$$
$$e_k = \{atr_h\},$$

где x_i – вершина метаграфа, $x_i \in X$;

e_i – ребро метаграфа, $e_i \in E$;

atr_j и atr_h – атрибуты вершин и ребер соответственно.

Таким образом, множества элементов программного обеспечения компьютерной сети и связей между элементами представляются следующим образом:

$X_1 = \{x_1^k\}$, $k = \overline{1,q}$ – множество ПО;

$X_2 = \{x_2^l\}$, $l = \overline{1,r}$ – множество ОС;

$X_3 = \{x_3^m\}$, $m = \overline{1,s}$ – множество ЛВС (подсетей);

$E_1 = \{e_1^n\}$, $n = \overline{1,t}$ – множество связей между ПО, определенных на множестве X_1;

$E_2 = \{e_2^o\}$, $o = \overline{1,u}$ – множество связей между ОС, определенных на множестве X_2;

$E_3 = \{e_3^p\}$, $p = \overline{1,v}$ – множество связей между ЛВС (подсетями), определенных на множестве X_3.

Тогда как вся компьютерная сеть будет составлять атрибутивный метаграф, или упорядоченную шестерку вида:

$$G = (X_1, X_2, X_3, E_1, E_2, E_3),$$

Причем существуют функции, обозначающие вхождение ПО в ОС и ОС в ЛВС:

$$f_1^w : g_1^w(x_1^k, e_1^n) \to x_2^l,$$

где x_1^k – элемент из множества программного обеспечения;

e_1^n – элемент из множества связей между программным обеспечением;

x_2^l – элемент из множества операционных систем.

$$f_2^y : g_2^y(x_2^l, e_2^o) \to x_3^m,$$

где x_2^l – элемент из множества операционных систем;

e_2^o – элемент из множества связей между операционными системами;

x_3^m – элемент из множества локальных вычислительных сетей.

Вершина характеризуется множеством атрибутов:

$$x_i^b = \{atr_a\},$$

где $i = \overline{1,3}$ – уровень вложенности вершины;

b – номер вершины на соответствующем уровне i;

atr_a – атрибуты вершины (числовые, строковые и др).

Ребро характеризуется множеством атрибутов:

$$e_i^h = \{x_i^s, x_i^e, \{atr_z\}\},$$

где x_i^c, x_i^d – связываемые ребром вершины;

$i = \overline{1,3}$ – уровень вложенности ребра;

atr_z – атрибуты ребра (числовые, строковые и т.д.);

Дополнительно вводится правило, что связь между двумя элементами на *i*-ом уровне существует тогда и только тогда, когда связь существует между всеми элементами, находящихся на более высоких уровнях, которым принадлежат объекты *i*-го уровня. Это означает что программное обеспечение, находящееся на разных операционных системах связано между собой только в том случае, если соответствующие операционные системы также связаны между собой.

С использованием разработанной модели возможно на этапе проектирования структуры систем учитывать характеристики элементов и взаимосвязи между ними для формирования требований к функциям средств защиты информации.

Предлагаемый подход к классификации угроз и разработанная ***модель угроз*** основаны на элементарных операциях над метаграфами. Как показано ранее компьютерная сеть рассматривается как структура из взаимодействующих элементов (вершины графа) и связей между ними (ребра графа). Под угрозами понимается несанкционированное изменение структуры компьютерной сети (графа).

На данном этапе необходимо обозначить, что в работе рассматриваются только угрозы безопасности системы, а не информации. При этом за основу берется классификация угроз по нарушаемым свойствам: конфиденциальность, целостность и доступность. Угрозы доступности для системы не рассматривается, так как при объединении перечней угроз безопасности информации и системы эти угрозы будут совпадать. Таким образом, рассматриваются угрозы целостности и конфиденциальности программного обеспечения компьютерной сети.

К базовым операциям над атрибутивными метаграфами относятся: добавление вершины или ребра; удаление вершины или ребра; изменение атрибута вершины или ребра.

На основе этого предлагаются следующие классы угроз целостности компьютерной сети:

1) Угрозы подмены элемента – C_{s1X};
2) Угрозы подмены связи – C_{s1E};
3) Угрозы удаления элемента – C_{s2X};
4) Угрозы удаления связи – C_{s2E};
5) Угрозы добавления элемента – C_{s3X};
6) Угрозы добавления связи – C_{s3E};
7) Угрозы изменения настроек элемента – C_{s4X};
8) Угрозы изменения настроек связи – C_{s4E}.

Угроза удаления элемента или связи характеризуется удалением вершины или ребра из множества X_i или E_j соответственно, так для множества ПО это характеризуется следующим образом:

$$G' = \left(X_1 \setminus x_1^k, X_2, X_3, E_1, E_2, E_3\right), \quad (1)$$

где X_1 – множество программного обеспечения;

x_1^k – удаляемое программное обеспечение, причем $x_1^k \in X_1$.

Угроза добавления элемента или связи характеризуется добавлением вершины или ребра из множества X_i или E_j соответственно, так для множества ПО это характеризуется следующим образом:

$$G' = \left(X_1 \cup x_1^{q+1}, X_2, X_3, E_1, E_2, E_3\right), \quad (2)$$

где x_1^{q+1} – добавляемое программное обеспечение.

Угроза подмены элемента или связи характеризуется удалением вершины или ребра из множества X_i или E_j соответственно и добавлением вершины или ребра вместо удаленного, т.е. для множества ПО это описывается последовательностью формул (1) и (2):

$$G' = \left(X_1 \setminus x_1^k, X_2, X_3, E_1, E_2, E_3\right),$$
$$G'' = \left(X_1 \cup x_1^{k\prime}, X_2, X_3, E_1, E_2, E_3\right).$$

Угроза изменения настроек элемента или связи осуществляется изменением атрибута вершины или ребра:

$$atr_a := atr_a'.$$

В качестве классификации угроз конфиденциальности компьютерной сети предлагаются следующие классы угроз:

1) Угрозы разглашения имени элемента – K_{s1X};
2) Угрозы разглашения имени связи – K_{s1E};
3) Угрозы разглашения настроек элемента – K_{s2X};
4) Угрозы разглашения настроек связи – K_{s2E}.

В теории графов угрозы конфиденциальности компьютерной сети описываются как пересечение множеств защищаемых элементов, информация о которых должна быть скрыта, с множествами общеизвестных элементов. Так, угроза разглашения (утечки) информации о имени программного обеспечения характеризуется пересечением множества X_1 с множеством J_1:

$$G' = (X_1 \cap J_1, X_2, X_3, E_1, E_2, E_3),$$

где $X_1 \cap J_1 = \left\{x_1^k \middle| x_1^k \in X_1 \wedge x_1^k \in J_1\right\}$;

x_1^k – элемент, принадлежащий множеству X_1;

X_1 – множество ПО, которое необходимо защитить;

J_1 – множество ПО, элементы которого известны всем.

Результатом работы является модель угроз компьютерной сети, которая объединяет все классы угроз K_S и C_S:

$$T_S = K_S \cup C_S;$$

где K_S – угрозы конфиденциальности элементов компьютерной сети;

C_S – угрозы целостности элементов компьютерной сети.

При этом, каждый из 12 представленных классов угроз содержит по 3 типа угроз: угрозы на уровне ПО, угрозы на уровне ОС и угрозы на уровне ЛВС – в общей сложности получается 36 типов угроз информационной безопасности программного обеспечения компьютерных сетей.

Недостатки, обозначенные в главе 1, были учтены и по возможности устранены:

1) элементы модели нарушителя полностью устранены из модели угроз;

2) все угрозы описаны однотипно, и присутствует строгое их разделение на классы;

3) угрозы были разделены на угрозы информации и системе, в настоящей рассмотрен подход к описанию угроз системе, т.е. компьютерной сети;

4) субъективность и влияние профессионального уровня эксперта при построении перечня угроз сведены к минимуму, благодаря формализации подхода к определению угроз.

Разработанная модель угроз позволяет составлять полные перечни угроз целостности и конфиденциальности компьютерных сетей.

С использованием вышеупомянутых моделей была разработана ***методика составления перечня угроз информационной безопасности*** компьютерных сетей, которая представляется 3 этапами:

1) классификация элементов компьютерной сети;
2) формирование матрицы взаимосвязей;
3) составление перечня угроз.

Функциональная схема методики в графической нотации IDEF0 представлена далее, на рисунке 1.

Входными данными для методики являются:

1) перечни прикладного и системного программного обеспечения;
2) логическая структура компьютерной сети;
3) перечень используемых протоколов передачи данных;
4) требования по учету угроз конфиденциальности и целостности в итоговом перечне угроз.

Результатом работы методики является перечень угроз информационной безопасности рассматриваемой компьютерной сети.

Механизмами управления являются модель компьютерной сети и модель угроз, описание которых представлено ранее.

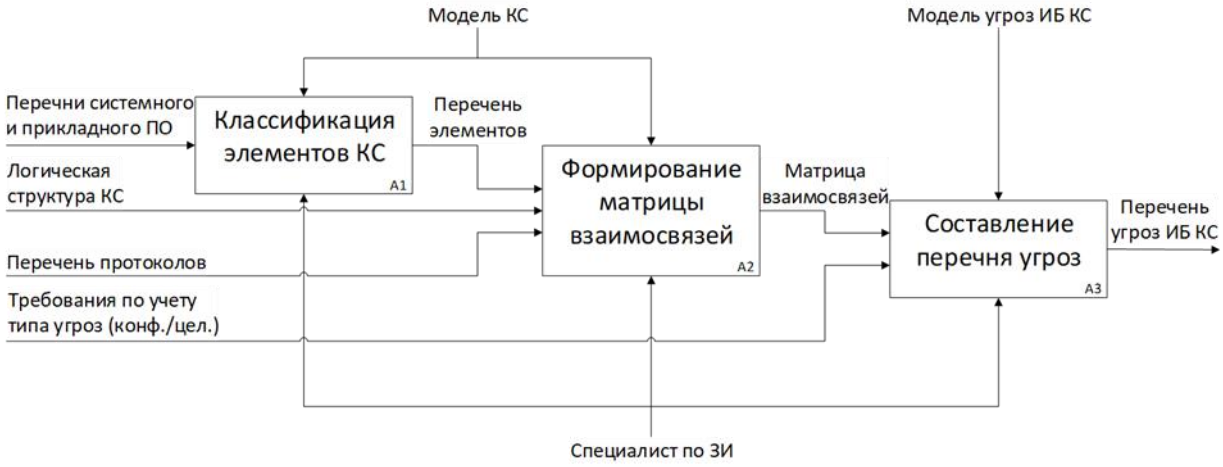

Рисунок 1 – Методика составления перечня угроз ИБ КС

Матрица взаимосвязей, использование которой является ключевой особенностью настоящей методики формируется следующим образом:

1) определяется перечень элементов компьютерной сети в соответствии с логической структурой сети;

2) определяется перечень использующихся протоколов;

3) сопоставляются перечни элементов и протоколов.

Перечень элементов подается на вход методики, однако в данном случае имеется в виду необходимость определить принадлежность элементов относительно иерархии: ЛВС включают ОС, а ОС, в свою очередь, включают ПО.

Перечень использующихся протоколов формируется из протоколов, с помощью которых осуществляется взаимодействие элементов в рамках рассматриваемой компьютерной сети.

Сопоставление перечней подразумевает определение того, с помощью каких протоколов взаимодействует каждая пара элементов. Все этапы формирования матрицы взаимосвязей могут осуществляться параллельно, однако для удобства разделены на последовательные шаги.

По своей сути матрица взаимосвязей представляет обозначение связей между элементами компьютерной сети аппаратом разработанной модели компьютерной сети в рамках методики.

Разработанная методика позволяет увеличить количество идентифицируемых угроз при формировании моделей угроз информационных систем и, в частности компьютерных сетей. Ее преимуществом является повторяемость: разные эксперты, используя ее, получат одинаковый перечень угроз для одной системы в независимости от их профессионального уровня. Однако, условием в данном случае будет правильное формирование перечня элементов рассматриваемой системы.

Третья глава посвящена сравнению разработанной модели угроз с наиболее полным аналогом, существующим на данный момент – банком данных угроз ФСТЭК России, а также апробации методики составления перечня угроз и моделей на реальном объекте – разрабатываемой автоматизированной системе коммерческого учета энергоресурсов.

В ходе ***сравнения*** была осуществлена классификация угроз информационной безопасности из банка данных угроз ФСТЭК России относительно объекта воздействия. Так как банк данных определяет угрозы, как нарушающие конфиденциальность, целостность и доступность информации, то возникают трудности при выделении среди них угроз информационной системе. Угрозы относились к угрозам системе в случае однозначного обозначения в описании угрозы, что она нарушает какое-либо из свойств системы. Угрозы, в описании которых значилось нарушение свойств информации вследствие получения доступа к системе считались угрозами информации. В итоге было выделено 68 угроз безопасности информационной системы. Все эти угрозы были соотнесены с выделенными в ходе разработки модели угроз типами.

Обобщенный результат сравнения представлен в таблице 1. Пересечения строк с классами угроз авторской модели со столбцами, в

которых обозначены уровни программного обеспечения компьютерной сети, обозначают выделенные типы угроз. Закрашенная ячейка значит, что в банке данных угроз ФСТЭК России были найдены угрозы информационной безопасности системы, относящиеся к данному типу, не закрашенная ячейка значит, что угроз, которые могли бы быть отнесены к данному типу обнаружено не было.

Таблица 1 – Сопоставление угроз из банка данных угроз ФСТЭК России с типами угроз авторской модели угроз

Классы угроз	Уровни программного обеспечения компьютерной сети		
	Уровень ПО	Уровень ОС	Уровень ЛВС
K_{s1X}			
K_{s1E}			
K_{s2X}			
K_{s2E}			
C_{s1X}			
C_{s1E}			
C_{s2X}			
C_{s2E}			
C_{s3X}			
C_{s3E}			
C_{s4X}			
C_{s4E}			

По результатам сравнения установлено, что предложенный подход к построению модели угроз позволяет специалистам по защите информации учесть при построении системы защиты информации на 11 типов угроз информационной безопасности системы больше, чем использование банка данных угроз ФСТЭК России. Всего согласно авторской классификации выделено 36 типов угроз конфиденциальности и целостности системы, в банке данных угроз ФСЭК России представлено 25 из них.

Результаты диссертационной работы ***были внедрены*** в деятельность АО «ПКК Миландр» в процессе работы над автоматизированной системой коммерческого учета энергоресурсов (АСКУЭ).

Для представления АСКУЭ, состоящей из трех основных типов элементов (устройство учета энергоресурсов (УУЭ), устройство сбора и передачи информации (УСПД), центральный сервер (ЦС)) была использована разработанная модель информационной системы на основе атрибутивных метаграфов. Ее использование позволило учесть при построении структуры АСКУЭ характеристики элементов и взаимосвязи между ними.

При применении методики и моделей к АСКУЭ рассматривались не уровни системы, обозначенные в главе 2 диссертационной работы, а программный и аппаратный уровни системы. К программному уровню АСКУЭ были отнесены операционные системы и программное обеспечение устройств, протоколы высокого уровня, программы конфигурирования

устройств. К аппаратному уровню системы отнесены все устройства системы, линии связи и протоколы низкого уровня.

Согласно разработанной модели двухуровневую систему можно представить как совокупность множества устройств X_1, в которое входят ЦС, а также все УСПД и УУЭ; множества программного обеспечения устройств X_1; множества связей на аппаратном уровне E_2; множества связей на программном уровне E_1. Расположение программного обеспечения на аппаратных компонентов будет обозначаться функциями вида:

$$f_1^1 : g_1^1(\text{"ПО ЦС"}_1^1) \rightarrow \text{"ЦС"}_2^1.$$

Соответственно вся система будет представлена следующим образом:

$$G = (X_1, X_2, E_1, E_2).$$

Также у каждого элемента системы есть характеризующие его параметры, представляемые атрибутами метаграфа. Графическое представление простейшей структуры АСКУЭ, описанной в понятиях авторской модели, представлено на рисунке 2.

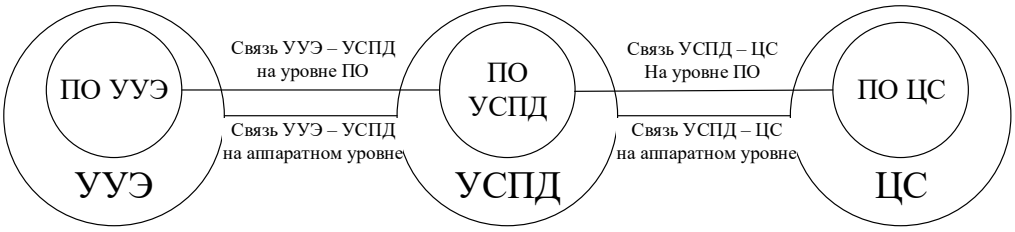

Рисунок 2 – Графическое представление модели АСКУЭ

После описания системы с помощью разработанной методики было осуществлено составление перечня угроз. При рассмотрении АСКУЭ заказчиком была поставлена задача определить угрозы целостности системы.

В результате был составлен перечень из 70 угроз целостности системы. Угрозы рассматривались на программном и аппаратном уровнях для трех основных типов элементов системы и связей между ними. Полученный с использованием авторской методики и моделей перечень оказался на 18% больше составленного экспертами заказчика ранее (59 угроз целостности системы).

В список не учтенных ранее угроз вошло 7 угроз целостности системы на аппаратном уровне и 4 угрозы целостности системы на программном уровне:

1) несанкционированное добавление УУЭ или УСПД в систему;
2) несанкционированное добавление УСПД или ЦС в систему;
3) использование несанкционированной аппаратной линии связи между УУЭ и УСПД;
4) использование несанкционированной аппаратной линии связи между УСПД и ЦС;
5) создание несанкционированных аппаратных связей между компонентами УУЭ;
6) создание несанкционированных аппаратных связей между комп. УСПД;

7) создание несанкционированных аппаратных связей между комп. ЦС;

8) подмена УУЭ или УСПД (в логической сети);

9) подмена УСПД или ЦС (в логической сети);

10) использование несанкционированного драйвера или протокола для связи между УУЭ и УСПД;

11) использование несанкционированного драйвера или протокола для связи между УСПД и ЦС.

Актуальность угроз в рамках данной работы не рассматривается, однако необходимо заметить, что получение хотя бы одной дополнительной угрозы, для которой необходимо вводить механизмы защиты, уже является достаточным основанием для рассмотрения расширенного перечня угроз. Это позволяет учесть при проектировании системы защиты необходимость дополнительных механизмов защиты.

В заключении приведены основные результаты и выводы по проделанной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате выполненного диссертационного исследования в области разработки моделей классификации угроз нарушения информационной безопасности была решена научно-техническая задача увеличения полноты перечня угроз информационной безопасности компьютерных сетей. Поставленная в начале исследования цель достигнута. Получены следующие основные результаты:

1) выполнен анализ текущего состояния предметной области: моделей компьютерных сетей, использующихся при идентификации угроз, а также подходов к построению моделей угроз компьютерных сетей. Были выделены их недостатки, требующие устранения;

2) на основе атрибутивных метаграфов разработана модель компьютерной сети, позволяющая описать компоненты программного обеспечения компьютерных сетей (прикладное, системное и сетевое программное обеспечение) и все возможные связи между ними (сетевые протоколы, драйверы, и т.п.);

3) на основе элементарных операций над метаграфами разработана модель угроз компьютерной сети, которая позволяет составлять полные перечни угроз целостности и конфиденциальности компьютерных сетей;

4) с использованием созданных моделей разработана методика составления перечня угроз информационной безопасности компьютерных сетей, отличающаяся от аналогов использованием матрицы взаимосвязей между элементами и позволяющая увеличить количество идентифицируемых угроз при формировании моделей угроз компьютерных сетей;

5) методика и модели были апробированы на практике в процессе разработки автоматизированной системы коммерческого учета

энергоресурсов, в результате чего было определено на 18% угроз целостности системы больше, чем до применения авторской методики.

Факт успешного внедрения методики составления перечня угроз информационной безопасности компьютерных сетей в деятельность АО «ПКК Миландр» в процессе разработки автоматизированной системы коммерческого учета энергоресурсов подтверждается актом внедрения. Также результаты диссертационного исследования используются в учебном процессе ФГБОУ ВО ТУСУР, что подтверждается актом внедрения.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ РАБОТЫ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

1. Новохрестов А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2016. – Т. 19. – № 3. – С. 111-114. – DOI: 10.21293/1818-0442-2016-19-3-111-114

2. Новохрестов А.К. Модель угроз безопасности информации и ее носителей / А.К. Новохрестов, А.А. Конев, А.А. Шелупанов, Н.С. Егошин// Вестник Иркутского государственного технического университета. – 2017. – Т. 21. – №12(131). – С. 93–104. – DOI: 10.21285/1814-3520-2017-12-93-104

В других изданиях, сборниках трудов и тезисов конференций:

3. Новохрестов А.К. Анализ состава сетевых средств защиты информации / А.К. Новохрестов, А.А. Конев // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: Материалы VI Межрегиональной научно-практической конференции. – Брянск: Изд-во БГТУ, 2014. – С. 93-96

4. Новохрестов А.К. Оценка качества защищенности сетей / А.К. Новохрестов // Научная сессия ТУСУР-2014: Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. – Томск: В-Спектр, 2014. - В 5 частях. – Ч. 3. – С. 208-210.

5. Новохрестов А.К. Классификация сетевых механизмов защиты / А.К. Новохрестов // Инновации и научно-техническое творчество молодежи: Российская научно-техническая конференция: Материалы конференции. – Новосибирск: Изд-во СибГУТИ, 2014. – С. 246-248.

6. Конев А.А. Методика оценки качества защищённости компьютерных сетей / А.А. Конев, А.К. Новохрестов // Проблемы информационной безопасности государства, общества и личности: Материалы XV всероссийской научно-практической конференции: Доклады VI Пленума

СибРОУМО по образованию в области информационной безопасности и XV конференции – Томск: В-Спектр, 2014. – С. 182-187.

7. Новохрестов А.К. Оценка качества защищенности компьютерных сетей / А.К. Новохрестов, А.А. Конев // Динамика систем, механизмов и машин: Материалы XI Международной научно-технической конференции. – Омск: Издательство ОмГТУ, 2014. – №4. – С. 85-87

8. Новохрестов, А.К. Использование методов и инструментальных средств управления рисками при оценке защищенности компьютерных сетей / А.К. Новохрестов // Научная сессия ТУСУР-2015: Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых (Томск, 13–15 мая 2015г.). – В 5 ч. – Ч. 4. – Томск: В-Спектр, 2015. – С. 172-173.

9. Новохрестов А.К. Многоуровневая модель информационной системы на основе атрибутивных метаграфов / А.К. Новохрестов, А.А. Конев // Электронные средства и системы управления: Материалы докладов XI Международной научно-практической конференции (25–27 ноября 2015 г.): В 2 ч. – Ч. 2. – Томск: ТУСУР, 2015. – С. 184-188.

10. Новохрестов А.К. Математическая модель угроз информационной системе / А.К. Новохрестов, А.А. Конев // Перспективы развития фундаментальных наук: Сборник трудов XIII Международной конференции студентов, аспирантов и молодых ученых. – Томск: НИ ТПУ, 2016. – С. 99-101.

11. Новохрестов А.К. Угрозы целостности информационной системы на уровне локальных вычислительных сетей / А.К. Новохрестов // Научная сессия ТУСУР-2016: Материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых. – В 6 частях. – Ч. 5. – Томск: В-Спектр, 2016. – С. 81-83.

12. Novokhrestov A. Mathematical model of threats to information systems / A. Novokhrestov, A. Konev // 13TH International conference of students and young scientists on prospects of fundamental sciences development: AIP conference proceedings (Tomsk, 26-29 April 2016). Vol. 1772. – Tomsk: AIP, 2016. – P. 060015. – DOI: 10.1063/1.4964595

13. Новохрестов А.К. Модель угроз конфиденциальности информационной системы / А.К. Новохрестов // Электронные средства и системы управления: Материалы докладов XII международной научно-практической конференции (16–18 ноября 2016 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр, 2016. – №1-2. – С. 56-58.

14. Степанова Т.С. Механизмы защиты информации от угроз компьютерным системам / Т.С. Степанова, А.К. Новохрестов // Студенческая наука для развития информационного общества: Сборник материалов V всероссийской научно-технической конференции. – Ставрополь: Изд-во СКФУ, 2016. – С. 497-500.

15. Новохрестов А.К. Обзор подходов к построению моделей информационной системы и угроз ее безопасности / А.К. Новохрестов, А.А.

Конев // Актуальные проблемы обеспечения информационной безопасности: Труды Межвузовской научно-практической конференции. – Самара: Инсома-Пресс, 2017. – С. 151-155.

16. Новохрестов А.К. Модель классификации угроз нарушения безопасности компьютерных сетей / А.К. Новохрестов, Т.С. Степанова // Электронные средства и системы управления: Материалы докладов XIII Международной научно-практической конференции (29 ноября – 1 декабря 2017 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр, 2017. – С. 76–79

Тираж 100 экз. Заказ _____.

Томский государственный университет
систем управления и радиоэлектроники

634050, г. Томск, пр. Ленина, 40.
Тел. (3822) 53-30-18.