Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

На правах рукописи

УДК 658.511.3

ФИЛИППОВА
Екатерина Александровна

АЛГОРИТМ ПРОВЕДЕНИЯ АНАЛИЗА И ОЦЕНКИ УЯЗВИМОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ОРГАНИЗАЦИИ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологии

по специальности 1-39 81 01-Компьютерные технологии
проектирования электронных систем

Минск 2016

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Цырельчук Игорь Николаевич,** заведующий кафедрой проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент

Рецензент: **Полубок Владислав Анатольевич,** заведующий кафедрой Микропроцессорных систем и сетей учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент

Защита диссертации состоится «24» июня 2016 г. года в $9^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П.Бровки, 6, 1 уч. корп., ауд. 415, тел.: 293-20-80, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

СОГЛАСОВАНО:
_____И.Н. Цырельчук
«___» _____ 2016 г.

ВВЕДЕНИЕ

На сегодняшний день автоматизированные системы (АС) играют ключевую роль в обеспечении эффективного выполнения бизнес-процессов как коммерческих, так и государственных предприятий. Вместе с тем повсеместное использование АС для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой. Подтверждением этому служит тот факт, что за последние несколько лет имеет место тенденция увеличения числа информационных атак, приводящих к значительным финансовым и материальным потерям.

Новые информационные технологии, глобальная компьютеризация и информационно-вычислительные сети, облачные вычисления породили новые источники угроз для всей информационной среды, в которой существует и развивается современное общество. Сегодня информационным атакам подвергаются различные объекты: экономические, объекты управления, оборонные системы, критически важные технологические объекты и т.п. Появились новые объекты защиты, на которые не обращалось практически никакого внимания в недавнем прошлом, например, персональные данные.

Быстрое развитие корпоративных сетей предприятий и организаций, позволяющих хранить всю информацию по персональным данным сотрудников. Нуждаются в особой системе защиты. Воздействия через глобальные информационные сети возрастает вместе с увеличением объемов информации, циркулирующей в сетях, а также информационных ресурсов, используемых при современном автоматизированном управлении организационными и организационно-техническими системами. В том числе и системами управления организациями. Ранее при решении задач защиты процессов, сопровождающих хранение, передачу и обработку информации, приходилось иметь дело с локальными объектами и с локальными угрозами безопасности их функционирования. Сейчас через сети распределения информации, особенно глобальные сети можно разрушить все информационные связи сразу. При этом информационная агрессия может начинаться так, что никто не узнает, откуда она исходит. Угроза становится анонимной. Явно обозначенный противник отсутствует, а его информационные атаки приносят значительный ущерб. В том числе информационным системам организации, содержащим персональные данные, данные о финансовом обеспечении как отдельно взятых проектов организации, так и зарплатной системы и системы материального стимулирования сотрудников.

В связи с постоянно нарастающими темпами развития средств вычислительной техники пропорционально возрастает уязвимость автоматизированных систем.

По этой причине в связи с ростом количества информационных атак в настоящее время проблема защиты информационно-программного обеспечения автоматизированных систем стала одной из злободневных и самых ключевых.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность диссертационного исследования

Каждое предприятие оснащено компьютерной техникой и доступом к глобальной сети *Internet*. Злоумышленники умело подключаются практически к каждой составной этой системы и с помощью многочисленного арсенала (вирусы, вредоносное ПО, подбор паролей и другое) воруют ценную информацию. Именно поэтому система информационной безопасности должна внедряться в каждую организацию без исключения.

Обеспечение информационной безопасности организации является одним из приоритетных направлений деятельности руководства в настоящее время. Очевидно, что надежность защиты информации напрямую зависит от ее ценности. Для защиты информации организации требуется комплекс мер, образующих систему. В теории под системой защиты информации понимают рациональную совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Элементами такой системы являются меры правового, организационного, технического и др. характера.

Таким образом, актуальность исследований по данной тематике заключается в анализе и оценке уязвимости автоматизированных систем в организации, а также снижение уязвимости системы обеспечения безопасности информации в организации.

Степень разработанности проблемы

На настоящий момент существует достаточно большое количество работ отечественных исследователей, рассматривающих анализ и оценку уязвимости систем защиты информационной безопасности, а также содержащих результаты исследований методов и средств снижения уязвимости автоматизированной систем (Асмолов Т.А., Политов М.С., Азаров А.А.). В рамках данной работы констатируется, что для существующего состояния теории и практики обеспечения безопасности применительно к особенностям функционирования организации имеет место противоречие между позитивными возможностями для эффективного функционирования системы управления организацией, которые несет за собой процесс автоматизации и информатизации всех процессов организации, и ростом рисков и угроз информационной безопасности организации посредством увеличения уязвимостей информационных систем организации.

Цели и задачи исследования

Цель исследования состоит в снижении уязвимости системы обеспечения безопасности информации в организации.

Для достижения поставленной цели решались следующие задачи:

1. Провести системный анализ уязвимости системы обеспечения информационной безопасности организации.

2. Разработать концепцию информационно-лингвистического анализа системы обеспечения безопасности информации в организации в терминах информационных взаимосвязей. Данная концепция должна затем быть использована в работе для разработки алгоритма проведения анализа и оценки уязвимости автоматизированных систем организации.

3. Спланировать методологическую основу для выполнения детализированного анализа информационной и функциональной взаимосвязи элементов системы обеспечения информационной безопасностью организации.

Область исследования

Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых по изучению оценки и анализа уязвимости системы защиты информационной безопасности.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна и достоверность полученных результатов

Научные новизна заключается разработке концепции информационно-лингвистического анализа системы обеспечения безопасности информации в организации в терминах информационных взаимосвязей.

Теоретическая значимость заключается в том, что проведенный анализ потенциальных угроз и предложенные системы защиты от них углубляют и расширяют общее содержание теории защиты информации применительно к организации. Полученные результаты систематизируют сведения теории защиты информации для организаций с учетом особенностей их функционирования.

Практическая значимость научных результатов исследований состоит в том, что они:

– позволяют за счет выявления множества критичных для безопасности организации элементов и связей между ними принимать меры к снижению уязвимости в среднем на 45-65%;

– позволяют включать в анализ схем информационных потоков такие операции как добавление в систему и удаление из нее компонентов;

– на их основе могут быть сформулированы новые критерии принятия решения о целесообразности того или иного усовершенствования АС.

Основные положения, выносимые на защиту

1. Перечень потенциальных угроз информационной безопасности организации и классификация методов их парирования.

2. Алгоритмы проведения анализа и оценки уязвимости автоматизированных организации.

3. Рекомендации по снижению уязвимости системы обеспечения безопасности информации в организации.

Апробация и внедрение результатов исследования

Основные результаты диссертационной работы общетеоретического и прикладного характера были внедрены:

– в ОАО “ПРОМСВЯЗЬ» (акт внедрении от 23.03.2016 года);

– в УО «БГУИР» (акт внедрении от 28.10.2015 года).

Результаты работы были представлены на 52-ой научной конференции аспирантов, магистрантов и студентов БГУИР, в журнале «Высшая Школа», в журнале «Научный Обозреватель».

Публикации

Основные положение диссертации и результаты исследования изложены в восьми опубликованных работах общим объемом 20 страниц.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения и библиографического списка.

В первой главе рассматривается понятие уязвимости АС. **Во второй главе** разрабатываются алгоритмы проведения анализа и оценки уязвимости автоматизированных систем организации. **В третьей главе** рассматривается применение разработанного во второй главе математического аппарата к организации с учетом применения рекомендаций по снижению уязвимости системы обеспечения безопасности информации организации. **В приложении** представлены публикации автора, акты внедрения и графическая часть.

Общий объем диссертации составляет 130 страниц, из них основного текста диссертации – 85. Работа содержит 51 рисунок, список использованных источников включает 79 наименования, список собственных публикаций соискателя из 6 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка использованной литературы.

Во **введении** рассмотрено современное состояние проблемы уязвимости автоматизированных систем, указаны основные направления исследований, проводимых в мире по данной тематике, а также описано обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** обоснована актуальность темы, определены цели и задачи диссертации, сформулирована научная новизна, основные вопросы исследования, практическая ценность и результаты, выносимые автором на защиту.

В **первой главе** рассматривается понятие уязвимости АС.

Данная работа была выполнена на базе открытого акционерного общества «ПРОМСВЯЗЬ».

ОАО «ПРОМСВЯЗЬ» представляет собой крупную организацию, с разветвленными структурой и системой управления, многочисленными пересекающимися информационными потоками.

На рисунке 1 представлена схема информационных потоков ОАО «ПРОМСВЯЗЬ».

Во **второй главе** разрабатываются алгоритмы проведения анализа и оценки уязвимости автоматизированных систем организации.

Алгоритм проведения анализа уязвимости автоматизированных систем организации:

1. Составляется список всех элементов АС (таблица 1):

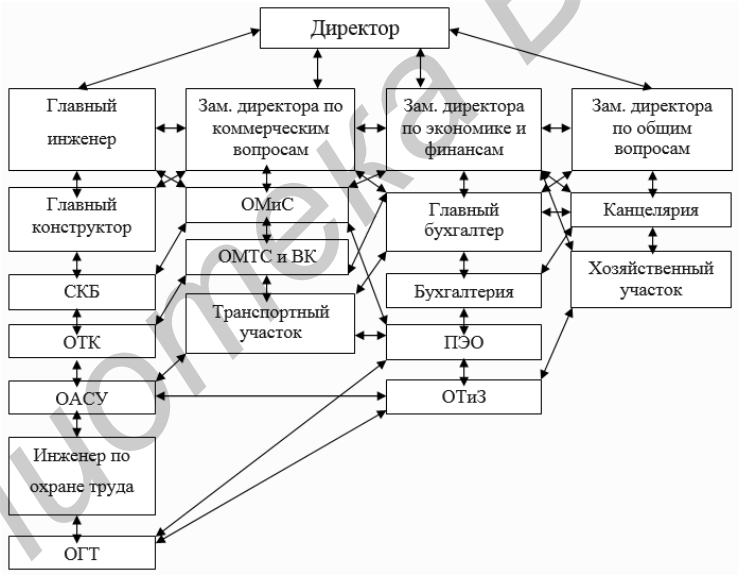

Рисунок 1 – Схема информационных потоков ОАО «ПРОМСВЯЗЬ»

Таблица 1 – Форма таблицы всех элементов АС

№ п/п	Название элемента, перечень составляющих его элементов
1.	Элемент А
2.	Элемент Б
. . .	. . .
N	Элемент Я

2. Для каждого элемента по шаблонам строятся (определяются) информационно-лингвистические схемы. Результаты табулируются в виде таблицы 2.

Таблица 2 – Результаты информационно-лингвистических схем

№ п/п	Название элемента, перечень составляющих его компонентов	ОФС	ИЛС
1.	Элемент А	ОФС элемента А	ИЛС элемента А
2.	Элемент Б	ОФС элемента Б	ИЛС элемента Б
. . .	. . .	. . .	. . .
N	Элемент Я	ОФС элемента Я	ИЛС элемента Я

3. В рамках исходных данных определяются тип, виды и информативность связей между элементами. В частном случае (таблица 3):

Таблица 3 – Информационная связь между элементами НИ

Тип элемента, от которого направлена связь	Чем определяется информативность связи
Элемент – объект доступа *j*	к скольким компонентам и НИ элемента i можно получить доступ, получив доступ к элементу j или(и) о скольких компонентах и НИ элемента i можно получить информацию вида C_{i_j} получив доступ к элементу j.
Элемент – субъект доступа *j*	к скольким компонентам и НИ элемента i имеет доступ элемент j12 или(и) о скольких компонентах и НИ элемента i элемент j владеет информацией вида C_{i_j}.

Информативность связи, направленной от элемента i к элементу j, обозначается индексированным символом h_{ij} и определяется по выражению (1):

$$h_{ij} = \frac{n_{ij}}{n_j}, \qquad (1)$$

где n_{ij} – число компонентов и носителей информации в ИЛС j-го элемента, определяемых связью, направленной от элемента i к элементу j (n_{ij} = 0,1,2,…,n_j);

n_j – общее число компонентов и носителей информации, определяемых ИЛС j- го элемента.

Результаты анализа АС табулируются в матричном виде.

С помощью подпрограммы автоматизации процесса формализации результатов контроля защищенности информации строится ориентированный граф, узлы (вершины) в котором это элементы АС, а ребра связи между ними.

Алгоритм проведения оценки уязвимости автоматизированных систем управления организации:

1. Строится А – матрица булевых коэффициентов $a_{m,k}$, единичные значения которых построчно определяют для каждого элемента АС s_m вектор $\bar{V}(a_{m,k})$ элементов.

2. Определяется величина n_1 – число строк A – матрицы, все элементы в которых равны единицы.

3. Рассчитывается усредненное по всем элементам АС значение того, в какой мере несанкционированный доступ к элементу или(и) вывод его из строя влияет на возможность нарушения безопасного режима функционирования АС.

4. Рассчитывается усредненное по всем элементам значение того, в какой мере НСД к одному из элементов АС приводит к снятию неопределенности о всем АС (приводит к опосредованному НСД ко всем элементам АС).

5. Рассчитывается значение показателя уязвимости АС (2):

$$V = 1 - \left(1 - \frac{n_1}{N} - \left(1 - \frac{n_1}{N}\right) A_{ss}\right)(1 - Di). \qquad (2)$$

6. Определяется класс и подкласс уязвимости АС (таблица 4).

Таблица 4 – Классы и подклассы уязвимости АС

Классы и подклассы уязвимости АС		Формальные признаки класса / подкласса		Критерии сравнения АС в рамках одного класса / подкласса
1 класс	подкласс 1.1	$n1 = N$, ($A_{ss} = 1$ и $V = 1$)	$Di = 1$	По значению Di
	подкласс 1.2		$0 < Di < 1$	
	подкласс 1.3		$Di = 0$	
2 класс	подкласс 2.1	$0 < n1 < N$	$Di = 1$	По значениям A_{ss} и n_1
	подкласс 2.2		$0 < Di < 1$	По значениям A_{ss}, Di и $n1$
	подкласс 2.3		$Di = 0$	По значениям A_{ss} и $n1$
3 класс	подкласс 3.1	$n1 = 0$	$Di = 1 \rightarrow V = 1$	По значению A_{ss}
	подкласс 3.2		$0 < Di < 1$, $A_{ss_1} < A_{ss} < A_{ss_2}$, где $A_{ss_1} = \frac{N-1}{N}\left(1 + \frac{N-1}{N}\right)$ – значение A_{ss} при котором $n_1=1$; $A_{ss_2} = \frac{N-1}{N}$ – максимальное значение A_{ss} при котором возможно выполнение условия $n_1=0$	По значениям Di и A_{ss}
	подкласс 3.		$0 < Di < 1$, $1/N < A_{ss} < A_{ss_2}$	
	подкласс 3.4		$Di = 0$, $A_{ss_1} < A_{ss} < A_{ss_2}$	По значению A_{ss}
	подкласс 3.5		$Di = 0$, $1/N < A_{ss} < A_{ss_2}$	

В **третьей главе** рассматривается применение разработанного во второй главе матаппарата к организации с учетом применения рекомендаций по снижению уязвимости системы обеспечения безопасности информации организации.

Анализируемая схема АС отдела автоматизированных систем управления ОАО «ПРОМСВЯЗЬ» представлена на рисунке 2.

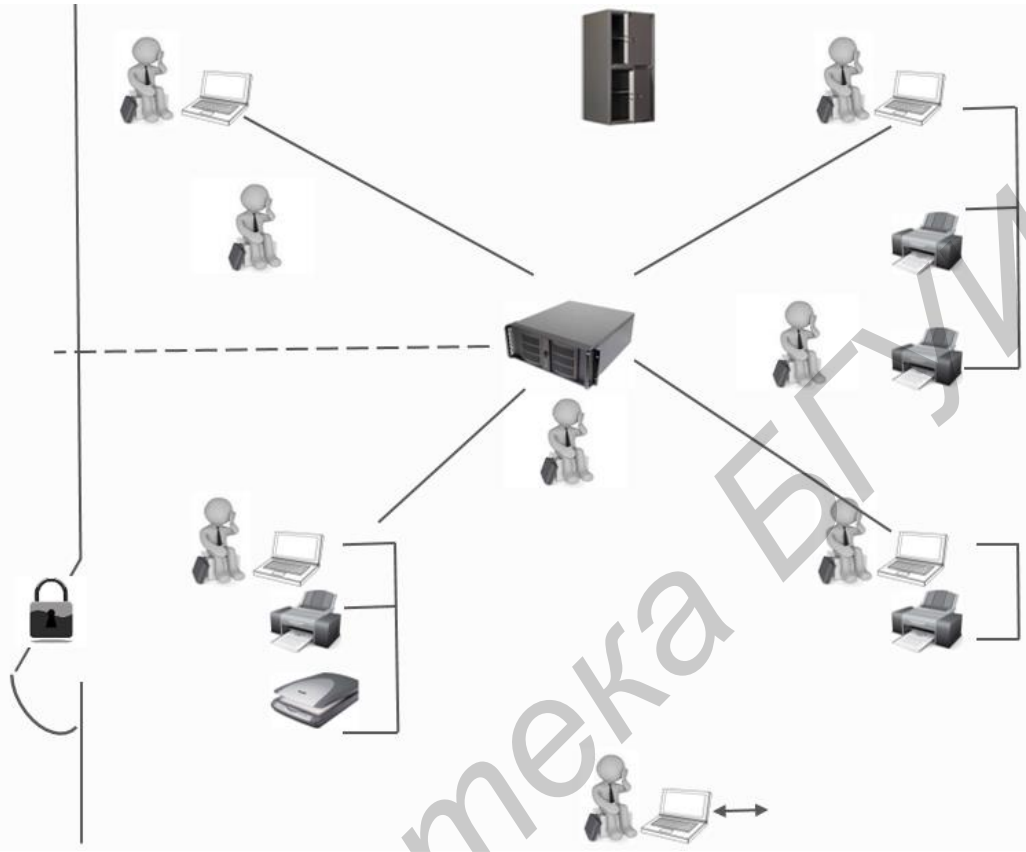

Рисунок 2 – Анализируемая схема АС отдела автоматизированных систем управления ОАО «ПРОМСВЯЗЬ»

В соответствии с рассмотренными выше алгоритмами были получены следующие результаты.

1) схема АС после ее логической фрагментации на множество субъектов доступа и относительно самостоятельные с точки зрения технической реализации и организации защиты информации элементы, каждый из которых имеет свои механизмы защиты информации, правила доступа, администрирования (рисунок 3);
2) список всех элементов АС с указанием для каждого объекта доступа ОФС и ИЛС;
3) матрица функциональной связности A_0;
4) матрица функциональной связности $A_{0,19;}$
5) таблица значений n;
6) таблица значений h_{ij};
7) таблица проконтролированных показателей.

В приведенным выше примере факт реализации рекомендаций визуализирован посредством выделения тех ячеек матриц A_0,$A_{0,19}$ и n_i, в которых в результате реализации рекомендаций произошло изменение ранее записанного значения.

Таким образом, применение рекомендаций позволила снизить показатель уязвимости системы на 60% и обеспечить более высокий подкласс уязвимости системы.

В **приложении** представлены слайды презентации на защиту магистерской диссертации и акты внедрения в производственный и учебный процессы, а также копии публикаций.

ЗАКЛЮЧЕНИЕ

Основные научные результаты работы:

1. Получен набор угроз безопасности и разрушения целостности информации организации ограниченного распространения, а также информационным ресурсам организации.
2. Классифицированы конкретные наборы методов и средств парирования различных видов угроз (от несанкционированного доступа, шпионажа и физических воздействий, электромагнитных излучений и наводок, компьютерных вирусов, взлома баз данных корпоративных систем организации).
3. Разработаны алгоритмы проведения анализа и оценки уязвимости автоматизированных систем организации.
4. Разработаны рекомендации по снижению уязвимости системы обеспечения безопасности информации в современном организации.
5. Получены теоретические и прикладные материалы использованы на базе ОАО «ПРОМСВЯЗЬ», что позволило повысить обоснованность и эффективность принимаемых управленческих решений по вопросам построения информационно-аналитической системы организации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Филиппова, Е.А. Организационные, физико-технические, информационные и программно-математические угрозы деятельности организации / Е.А. Филиппова // Научно-практический журнал «Высшая школа», №11 / 2016 – Уфа: Инфинити, 15 июня 2016 – С. 118.

2-А. Климович, Д. М., Исследование решений для приборов контроля электростатической безопасности человека / Д.М. Климович, Е.А. Филиппова // Научно-практический журнал «Высшая школа», №11 / 2016 – Уфа: Инфинити, 15 июня 2016 – С. 107.

3-А. Филиппова, Е.А. Концептуальные положения политики информационной безопасности в организации / Е.А. Филиппова // Научно-практический журнал «Научный обозреватель», №6 (66) – 2016 – Уфа: Инфинити, 23 июня 2016 – С. 63.

4-А. Климович, Д.М. Природа электростатического поля и его влияние на производство / Д.М. Климович, Е.А. Филиппова // Научно-практический журнал «Высшая школа», №11 / 2016 – Уфа: Инфинити, 15 июня 2016 – С.86 – 88.

5-А. Филиппова, Е.А. Алгоритм проведения анализа уязвимости автоматизированных систем управления организации / Е.А. Филиппова // Материалы работы 52-й научной конференции аспирантов, магистрантов и студентов БГУИР. – Минск: БГУИР, 25-30 апреля 2016 (в печати).

6-А. Филиппова, Е.А. Требования к формированию политики безопасности в организации / Е.А. Филиппова // Материалы работы 52-й научной конференции аспирантов, магистрантов и студентов БГУИР. – Минск: БГУИР, 25-30 апреля 2016 (в печати).

РЭЗЮМЭ

Філіпава Кацярына Аляксандраўна

Алгарытм правядзення аналізу і ацэнкі уразлівасці аўтаматызаваных сістэм у арганізацыі

Ключавыя словы: абарона інфармацыі, аўтаматызаваная сістэма бяспекі, уразлівасць сістэмы.

Мэта працы: зніжэнні слабыя месцы сістэмы забеспячэння бяспекі інфармацыі ў арганізацыі.

Навуковая навізна і дакладнасць атрыманых вынікаў: навізна заключаецца распрацоўцы канцэпцыі інфармацыйна-лінгвістычнага аналізу сістэмы забеспячэння бяспекі інфармацыі ў арганізацыі ў тэрмінах інфармацыйных узаемасувязяў.

Дакладнасць атрыманых вынікаў пацвярджаецца:

– выкарыстаннем пры правядзенні даследаванняў асноватворных канцэпцый і метадаў сучаснай матэматыкі, тэорыі графаў, а таксама ў базавых прыкладаннях тэорый верагоднасці і тэорый мностваў.

– збежнасць да вядомых выніках пры увядзенні абмежаванняў і дапушчэнняў;

– разглядам з адзіных метадалагічных пазіцый асноўных задач даследаванняў, якія ляжаць у аснове вырашаемай праблемы, што дазволіла аргументавана падысці да фармулёўкі мэты даследаванняў і прапанаваным да яе дасягнення падыходам.

Ступень выкарыстання: вынікі ўкаранёны на ААТ «Прамсувязь» і на кафедры Пікс ў навучальны працэс

Вобласць прымянення: на сённяшні дзень у інфармацыйнай бяспекі маюць патрэбу розныя аб'екты: эканамічныя, аб'екты кіравання, абарончыя сістэмы, крытычна важныя тэхналагічныя аб'екты і да т.п.

РЕЗЮМЕ

Филиппова Екатерина Александровна

Алгоритм проведения анализа и оценки уязвимости автоматизированных систем в организации

***Ключевые слова*:** защита информации, автоматизированная система безопасности, уязвимость системы.

***Цель работы*:** снижении уязвимости системы обеспечения безопасности информации в организации.

Научная новизна и достоверность полученных результатов: новизна заключается разработке концепции информационно-лингвистического анализа системы обеспечения безопасности информации в организации в терминах информационных взаимосвязей.

Достоверность полученных результатов подтверждается:

– использованием при проведении исследований основополагающих концепций и методов современной математики, теории графов, а также в базовых приложениях теорий вероятности и теорий множеств.

– сходимостью к известным результатам при введении ограничений и допущений;

– рассмотрением с единых методологических позиций основных задач исследований, лежащих в основе решаемой проблемы, что позволило аргументировано подойти к формулировке цели исследований и предложенным к ее достижению подходам.

***Степень использования*:** результаты внедрены на ОАО «ПРОМСВЯЗЬ» и на кафедре ПИКС в учебный процесс

***Область применения*:** на сегодняшний день в информационной безопасности нуждаются различные объекты: экономические, объекты управления, оборонные системы, критически важные технологические объекты и т.п.

SUMMARY

Filippova Ekaterina

Chart of the vulnerability analysis and evaluation of automated systems in organizations

Keywords: information security, automated security system vulnerability.

Objective: To reduce the vulnerability of information security in the organization.

Scientific novelty and reliability of the results: innovation is the development of the concept of information and linguistic analysis of the security of information systems in the organization of information in terms of relationships.

Reliability the results is confirmed:

– the use in research of fundamental concepts and methods of modern mathematics, graph theory, as well as basic applications of the theory of probability and set theory.

– convergence of the known results of the introduction of restrictions and assumptions;

– consideration of a uniform methodological positions of the main tasks of research, the underlying problem to be solved, allowing reasoned approach to the formulation of research objectives and proposed approach to achieve it.

Use level: the results are introduced at JSC "Promsvyaz" and at the department of educational process in the PICS

Scope: to date, the various objects in need of information security: economic, management objects, defense systems, mission-critical technology items, etc.