A.S. Zaytsev, A.A. Malyuk
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
31, Kashirskoe sh., Moscow, 114509, Russian Federation,
e-mail: Anthony.Zaytsev@gmail.com, e-mail: AAMalyuk@mephi.ru

Development of information security insider threat classification using incident clustering

Keywords: Clustering analysis of information security incidents, classification of information security insider threats
Effective information security insider threat countermeasure requires knowledge and understanding of actual insider threats and methods of their realization. The article represents analysis of existing insider threat's and intruder's classifications. This analysis elicited an absence of comprehensive and consistent classification nowadays. Basing of this outcome a method of insider threat classification development using clustering of incidents was introduced. For this purpose an insider incident database was created and filled with 500 open source incidents. For determination of classification criterions and criterions of result estimation an analysis of gathered statistics was carried out. Using modeling framework IBM SPSS Modeler incident clustering was conducted basing on the following algorithms: k-means, two-step clustering algorithm, Cohonen self-organizing maps. Basing on incident clustering an information security insider threat classification was developed.

А.С. Зайцев, А.А. Малюк
Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе,31,г. Москва, 115409, Россия,
e-mail: Anthony.Zaytsev@gmail.com, e-mail: AAMalyuk@mephi.ru

РАЗРАБОТКА КЛАССИФИКАЦИИ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ КЛАСТЕРИЗАЦИИ ИНЦИДЕНТОВ

Ключевые слова: кластерный анализ инцидентов информационной безопасности, классификация внутренних угроз информационной безопасности
Для эффективного противодействия внутренним нарушителям информационной безопасности необходимо знать и понимать актуальные внутренние угрозы и методы их реализации. В статье поведен анализ существующих классификаций внутренних угроз и нарушителей ИБ, выявивших отсутствие в настоящее время полной и непротиворечивой классификации. Ввиду этого предложен метод разработки классификации внутренних угроз информационной безопасности с использованием кластеризации инцидентов. Для этого разработана база внутренних инцидентов информационной безопасности, в которую вошло 500 инцидентов из открытых источников. Проведен анализ статистики инцидентов для определения критериев классификации, разработаны критерии оценки результатов кластеризации. Произведена кластеризация инцидентов с использованием среды моделирования IBM SPSS Modeler, реализующей различные алгоритмы кластеризации: k-средних, двухшаговый алгоритм кластеризации, самоорганизующиеся карты Кохонена. На основе кластеризации инцидентов получена классификация внутренних угроз ИБ.

Введение

Деятельность по обеспечению информационной безопасности (ИБ) включает в себя защиту от внутренних и внешних угроз. Защита от внешних угроз в достаточной мере обеспечивается организационными и технологическими средствами и методами, базирующимися на развитой системе стандартов и других руководящих и методических документов. Такие системы созданы сегодня как на национальном, так и на международном уровнях. Обеспечение ИБ в условиях реализации внутренних угроз изучено не настолько хорошо, и разработать полноценную методологию защиты информации от внутренних угроз только предстоит. Причем принципиальным моментом здесь является то, что проблема противодействия инсайдерской угрозе не технологическая, а скорее организационно-психологическая, и решение ее должно в значительной степени базироваться на исследовании гуманитарных аспектов ИБ.

А.С. Зайцев, А.А. Малюк

РАЗРАБОТКА КЛАССИФИКАЦИИ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ КЛАСТЕРИЗАЦИИ ИНЦИДЕНТОВ

Обеспечение ИБ в условиях реализации внутренних угроз можно представить как сочетание двух типов деятельности: предотвращение возникновения внутренних угроз и противодействие возникающим или возникшим внутренним угрозам ИБ. Противодействие внутренним угрозам ИБ состоит, в свою очередь, из обнаружения потенциального внутреннего нарушителя ИБ по проявляемым им поведенческим и техническим индикаторам и дальнейшего выбора и применения контрмер. Причем оба типа деятельности невозможно осуществлять без полноценной актуальной классификации внутренних угроз ИБ. Классификацию внутренних угроз ИБ целесообразно разрабатывать, опираясь на статистические данные по уже произошедшим инцидентам ИБ.

Целью данной статьи является разработка классификации внутренних угроз на основе кластерного анализа статистики инсайдерских инцидентов ИБ.

Анализ классификаций внутренних угроз и нарушителей информационной безопасности

Рассмотрим предлагаемые на сегодняшний день в различных источниках классификации внутренних нарушителей ИБ.

В [1] представлена классификация внутренних нарушителей, использующая в качестве критерия полномочия, которыми они пользуются в автоматизированной системе (АС). Данная классификация устанавливает 4 класса инсайдеров: от 1 класса – минимальные полномочия в АС (запуск фиксированного набора задач), до 4 класса – максимальные полномочия в АС, вплоть до включения в состав АС новых средств.

В [2] предложена приведенная в табл. 1 классификация внутренних нарушителей ИБ в зависимости от занимаемых ими должностей.

Таблица 1. Классификация инсайдеров в зависимости от занимаемой должности

Уровень риска	Пользователь
Наибольший риск	сетевой администратор; администратор безопасности.
Повышенный риск	оператор системы; оператор ввода и подготовки данных; менеджер обработки; системный программист.
Средний риск	инженер системы; менеджер программного обеспечения.
Ограниченный риск	прикладной программист; инженер или оператор по связи; администратор баз данных; инженер по оборудованию; оператор периферийного оборудования; библиотекарь системных магнитных носителей; пользователь-программист; пользователь-операционист.
Низкий риск	инженер по периферийному оборудованию; библиотекарь пользовательских магнитных носителей; пользователь сети.

Таким образом, как видим, в качестве критериев классификации в [1,2] используются возможности потенциального нарушителя в информационной системе (ИС) организации.

В [3] представлен несколько другой подход, на основе которого разработаны две классификации внутренних нарушителей ИБ. В первой, принадлежащей компании *IDC*, выделено 4 класса внутренних нарушителей ИБ: «граждане», «нарушители», «отступники» и «предатели». «Граждане» – лояльные сотрудники, не нарушающие принятые в организации

правила по обеспечению ИБ. «Нарушители» – сотрудники, соблюдающие правила по обеспечению ИБ, но позволяющие себе при случае их нарушить в незначительной степени. «Отступники» – сотрудники, не видящие проблемы в нарушении правил по обеспечению ИБ. Наконец, «Предатели» – сотрудники, сознательно идущие на серьезные нарушения, зачастую ввиду финансового вознаграждения «со стороны».

Вторая классификация из [3], разработанная компанией *Infowatch*, является наиболее полной (см. табл. 2).

Таблица 2. Классификация инсайдеров, разработанная Infowatch

Тип	**Умысел**	**Корысть**	**Постановка задачи**	**Действия при невозможности**
Халатный	Нет	Нет	Нет	Сообщение
Манипулируемый	Нет	Нет	Нет	Сообщение
Обида	Да	Нет	Сам	Отказ
Нелояльный	Да	Нет	Сам	Имитация
Подрабатывающий	Да	Да	Сам/Извне	Отказ/Имитация/Взлом
Внедренный	Да	Да	Извне	Взлом

Как видим, в качестве критериев классификации в [3] используются мотив нарушителя и наличие внешнего сговора.

Рассмотрим теперь существующие классификации внутренних угроз ИБ.

В [3] выделены следующие классы угроз:

1. Утечка конфиденциальной информации;
2. Обход средств защиты от утечки конфиденциальной информации;
3. Кража конфиденциальной информации по неосторожности;
4. Нарушение авторских прав на информацию;
5. Мошенничество;
6. Нецелевое использование информационных ресурсов компании;
7. Саботаж ИТ-инфраструктуры.

Данная классификация, очевидно, обладает следующими недостатками:

1. Классы «Обход средств защиты от утечки конфиденциальной информации», «Кража конфиденциальной информации по неосторожности», «Нарушение авторских прав на информацию» по сути является подклассами класса «Утечка конфиденциальной информации».

2. Угрозы неумышленного нарушения целостности и доступности информации и ИС организации не описываются данной классификацией.

3. Угроза шантажа руководства организации нарушением ИБ также не описывается данной классификацией.

В [4] выделены следующие классы угроз:

1. Саботаж ИТ-инфраструктуры;
2. Шпионаж;
3. Мошенничество на руководящей должности;
4. Мошенничество на не руководящей должности;
5. Кража интеллектуальной собственности для получения деловых преимуществ в одиночку;
6. Кража интеллектуальной собственности для получения деловых преимуществ с соучастниками;
7. Нарушение ИБ по халатности;
8. Социальная инженерия.

Данной классификации внутренних угроз ИБ свойственны следующие недостатки:

1. Класс угроз «Шпионаж» включает в себя только угрозу международного шпионажа, угрозу промышленного шпионажа предлагается рассматривать в рамках класса угроз «Мошенничество».

2. Некоторые угрозы, такие как продажа конфиденциальной информации на черном рынке или шантаж руководства организации нарушением конфиденциальности или целостности информации, не входят ни в один из приведенных классов.

Учитывая данные приведенного анализа, сформируем далее базу внутренних инцидентов (БВИ) ИБ и на основе этого статистического материала разработаем классификацию внутренних нарушителей и угроз ИБ.

Разработка базы внутренних инцидентов информационной безопасности

В первую очередь необходимо определить формат и программную реализацию БВИ. Требования к формату базы внутренних инцидентов ИБ выглядят следующим образом:

1. Формат базы должен учитывать формат существующих баз. В настоящий момент отсутствуют общедоступные базы инцидентов. Описание инцидентов со ссылкой на источник публикует компания *Infowatch*, но данные инциденты ограничены угрозой утечки конфиденциальной информации и не упорядочены в виде базы. Научный центр *CERT* в своих публикациях приводит формат используемых им БВИ для мотивированных[5] и немотивированных[6] внутренних инцидентов ИБ. Информация в базе мотивированных инцидентов *CERT* явно избыточна, а в базе немотивированных инцидентов – ее недостаточно. Однако представляется целесообразным использовать общий подход к формированию БВИ, предложенный *CERT*: «Портрет организации – Портрет нарушителя – Портрет инцидента».

2. В базе должны быть столбцы, представляющие общепринятые критерии классификации внутренних угроз и нарушителей ИБ. В существующих классификациях внутренних угроз и нарушителей ИБ в качестве критериев используются должность инсайдера, мотив инсайдера и тип внешнего сговора.

3. Информации в столбцах базы должно быть достаточно для однозначной идентификации инцидентов и поиска повторов.

4. В базе должны быть столбцы, используемые разрабатываемыми моделями (индикаторы и критерии классификации).

5. В базе должна быть информация об ущербе, причиненном инцидентом.

Требования к программной реализации базы:

1. Программная реализация базы должна позволять осуществлять автоматизированный поиск повторов, группировку инцидентов по определенным критериям, поверку достаточности критериев классификации.

2. База должна быть совместима с используемой средой моделирования.

Таким образом, итоговый формат разрабатываемой БВИ будет выглядеть так, как представлено в табл. 3.

Таблица 3. Формат базы внутренних инцидентов

Информация	**Столбец в базе**
Описание	Описание
Портрет организации	Название
	Страна
	Отрасль
Портрет инсайдера	Имя
	Пол
	Возраст

Информация	**Столбец в базе**
	Должность
	Продолжительность работы в компании до инцидента
	Преступное прошлое
Портрет инцидента	Мотив инсайдера
	Объект атаки (информация, ИТ-инфраструктура)
	Нарушенное свойство (конфиденциальность, целостность, доступность)
	Категория информации (при наличии)
	Внешний сговор
	Внутренний сговор
	Инициатор увольнения (при наличии)
	Длительность инцидента
	Ущерб организации
Индикаторы	Технические индикаторы
	Поведенческие индикаторы
Источник	Источник

В качестве инструмента для реализации БВИ использовалась программа *Microsoft Excel*, которая позволяет организовать хранение информации об инцидентах в виде таблиц и автоматизировано их обрабатывать при помощи встроенного языка программирования *Visual Basic for Applications* (*VBA*).

В рамках анализа статистической информации было исследовано более 1200 внутренних инцидентов ИБ, из которых 500 были достаточно информативны для добавления в БВИ. В качестве источников инцидентов выступали: отчеты научно-исследовательских организаций, аналитические сводки компаний, занимающихся противодействием внутренним угрозам ИБ, новостные сводки сайтов, посвященных ИБ, новостные сводки сайтов, посвященных ИТ, новостные ленты и СМИ, информационные сводки государственных структур, занимающихся борьбой с киберпреступностью и пр.

Подготовка данных для моделирования

Для разработки классификации внутренних угроз ИБ в статье решается математическая задача кластеризации инцидентов: разбить n m-мерных векторов на k кластеров. Прежде всего необходимо определить перечень критериев, по которым реализованные в инцидентах угрозы будут разбиты по классам угроз. Для моделей, решающих математическую задачу кластеризации, критерии выступают в роли предикторов – переменных, подающихся на вход модели.

Предикторов, с одной стороны, должно быть достаточно для однозначного определения каждого класс угроз, с другой стороны, их не должно быть слишком много, т.к. это может привести к нехватке статистических данных, требуемых для обучения.

Для формирования перечня критериев классификации инциденты из БВИ в первую очередь были разбиты на группы в зависимости от реализуемых угроз. Далее экспертным путем были определены критерии, однозначно описывающие каждую угрозу.

Перечень данных критериев классификации выглядит следующим образом:

- Мотив инсайдера;
- Внешний сговор;
- Внутренний сговор;
- Должность инсайдера;

- Объект атаки;
- Категория информации;
- Нарушенное свойство;
- Инициатор увольнения;
- Продолжительность преступления/правонарушения.

В целях проверки достаточности выбранных критериев классификации для однозначного определения каждой угрозы разработан макрос *VBA*, который осуществляет

перевод угроз в векторную форму (по критериям классификации) и поиск одинаковых векторов. По результатам работы макроса анализируется, относятся ли угрозы, описывающиеся одинаковыми векторами, предположительно к одному и тому же классу угроз. Если да, то набор критериев классификации является достаточным, если нет – необходимо его дополнить.

Оптимальное число критериев классификации было определено экспериментальным путем посредством тестового моделирования. Порядок и состав критериев классификации определены экспертным путем при помощи парных сравнений (табл. 4).

Таблица 4. Парные сравнения критериев классификации

Критерий	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Сумма**
Мотив (1)	1	1	2	1	1	1	1	2	2	12
Внешний сговор (2)	1	1	2	1	1	1	1	2	2	12
Внутренний сговор (3)	0,5	0,5	1	1	0,5	1	0,5	1	1	7
Должность (4)	1	1	1	1	1	1	1	1	1	9
Объект атаки (5)	1	1	2	1	1	1	1	2	2	12
Категория информации (6)	1	1	1	1	1	1	1	2	2	11
Нарушенное свойство (7)	1	1	2	1	1	1	1	1	1	10
Инициатор увольнения (8)	0,5	0,5	1	1	0,5	0,5	1	1	1	7
Продолжительность (9)	0,5	0,5	1	1	0,5	0,5	1	1	1	7

В качестве предикторов для модели отобраны критерии классификации, набравшие в сумме более 9 баллов. Предикторы в порядке их значимости в соответствии с таблицей парных сравнений будут следующими:

1. Мотив инсайдера;
2. Внешний сговор;
3. Объект атаки;
4. Категория информации (подвергнувшейся атаке);
5. Нарушенное свойство (конфиденциальность, целостность или доступность);
6. Должность инсайдера.

Каждая детальная угроза далее представляется в виде вектора с символическими координатами в соответствии с данными предикторами.

Результаты моделирования

Задача кластеризации решалась при помощи следующих методов и алгоритмов:

1. *k*-средних;
2. Двухшаговый алгоритм кластеризации (модификация алгоритма *BIRCH*);
3. Сеть Кохонена.

Для начала необходимо определить критерии оценки результатов моделирования. Модели кластеризации характеризуются следующими величинами [7]:

1. Значением силуэтной меры – меры оценки кластеров, определяющей близость векторов внутри кластеров и разделенность векторов между кластерами.
2. Рейтингом значимости использованных предикторов для кластеризации.
3. Размером минимального кластера.
4. Отношением размера минимального кластера к максимальному.

Для оценки результатов работы полученных моделей были выбраны следующие критерии оценки результатов:

1. Значение силуэтной меры (объективный критерий):

$$s = \sum_{i=1}^{n} \frac{B(x_i) \quad A(x_i)}{\max\left(A(x_i), B(x_i)\right)}$$

где $A(x_i)$ – расстояние от вектора x_i до центра кластера, к которому отнесен данный вектор, $B(x_i)$ – минимальное расстояние от этого вектора до центров остальных кластеров.

2. Совпадение значимости предикторов с экспертной оценкой (субъективный критерий).

Классификация внутренних угроз ИБ должна включать в себя:

1. Классы угроз.
2. Объединенные классы угроз.
3. Корреляцию с существующими классификациями угроз и нарушителей.
4. Риск, определенный как суммарный ущерб от инцидентов, определивших данный класс угроз (средний ущерб от инцидента в БВИ принимается в размере 6 840 000 рублей).

Для разработки моделей кластеризации использовалась среда моделирования *IBM SPSS Modeler* 16.0, в которой последовательность действий по обработке и анализу данных изображается в виде так называемого потока. Разработанный поток *SPSS Modeler* приведен на рис. 1. В левой части рисунка располагается источник данных (таблица *Excel*), которые подаются на вход кластеризаторов, изображенных в виде пятиугольников. Кластеризаторы формируют модели, изображенные в виде ограненных драгоценных камней, а данные по принадлежности инцидентов к кластерам сохраняются в таблице *Excel* (расположены в правой части рисунка).

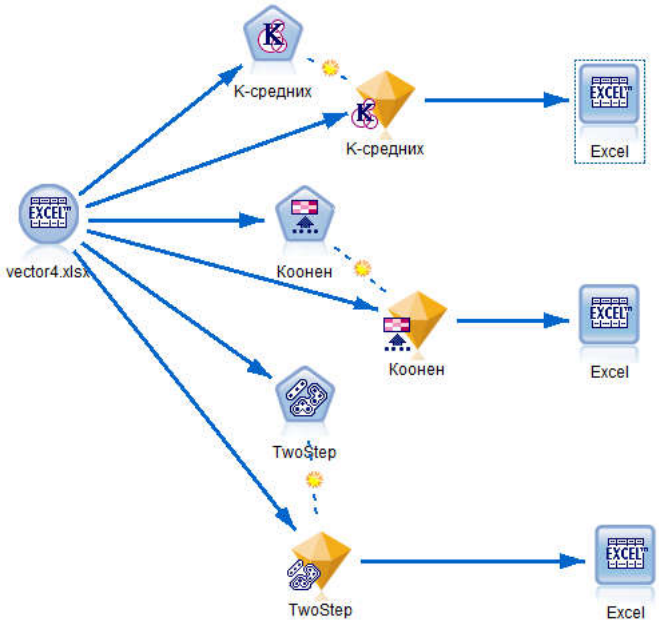

Рис. 1. Поток SPSS Modeler для кластеризации инцидентов

Оценка результатов работы моделей приведена в табл. 5.

Таблица 5. Оценка результатов работы моделей

Алгоритм/метод	**Значение силуэтной меры**	**Совпадение важности предикторов с экспертной оценкой**
k-средних	0,5	3
Двухшаговый алгоритм	0,5	1
Сеть Кохонена	0,2	3

Сравнение важности предикторов приведено в табл. 6.

Таблица 6. Сравнение важности предикторов

Экспертная оценка	**К-средних**	**Двухшаговый алгоритм**	**Сеть Кохонена**
*С*2 *С*3 *С*5	*С*6	*С*6	*С*3
*С*2 *С*3 *С*5	*С*3	*С*3	*С*2
*С*2 *С*3 *С*5	*С*2	*С*7	*С*6
*С*6	*С*7	*С*4	*С*7
*С*7	*С*5	*С*2	*С*5
*С*4	*С*4	*С*5	*С*4

В таблице использованы следующие обозначения: С2 – мотив, С3 – внешний сговор, С4 – должность, *С*5 – объект атаки, *С*6 – категория информации, *С*7 – нарушенное свойство.

В результате по выбранным критериям оценки лучшие результаты показал алгоритм *k*-средних.

Ввиду того, что часть критериев классификации была отсеяна на этапе выбора предикторов, полученные классы угроз не дифференцированы по следующим критериям: внутренний сговор, продолжительность противоправных действий, инициатор увольнения. Данные критерии классификации учтены экспертным путем. Полученная классификация внутренних угроз ИБ приведена в табл. 7.

Таблица 7. Классификация внутренних угроз информационной безопасности

Мотив инсайдера	**Объединенный класс угроз**	**Класс угроз**	**Соответствующий класс классификации CERT**	**Риск, руб.**
Идея	Идейное нарушение ИБ	Нарушение конфиденциальности ИОД из идейных соображений	Нет	479 610 000
Нет	Халатное нарушение ИБ	Ошибка конфигурации	Халатное нарушение ИБ	65 580 000
		Потеря носителя ИОД		105 254 680 000
		Неправильная утилизация носителя ИОД		47 880 000
		Непреднамеренное разглашение ИОД		143 640 000
	Социальная инженерия	Социальная инженерия	Социальная инженерия	205 500 000
Обида	ИТ-саботаж	Установка логической бомбы	ИТ-саботаж	152 430 000
		Диверсия ИТ-инфраструктуры при удаленном подключении		214 131 000
		Продолжительное		9 080 000

Мотив инсайдера	**Объединенный класс угроз**	**Класс угроз**	**Соответствующий класс классификации CERT**	**Риск, руб.**
		вредительство		
		Удаление информации		89 580 000
		Изменение конфигурации или порча оборудования		28 860 000
Деньги	Шпионаж	Кража ИОД для открытия своего дела или перехода к конкуренту	Кража интеллектуальной собственности для получения деловых преимуществ	26 570 360 000
		Разовая кража ИОД в интересах конкурента	Шпионаж, мошенничество на не руководящей должности	30 813 845 000
		Продолжительная кража ИОД в интересах конкурента		65 068 760 000
	Манипулирование рынком	Неправомерное использование инсайдерской информации для манипулирования рынком	Нет	3 465 990 000
	Мошенничество	Мошенничество с банковскими картами	Мошенничество на не руководящей должности	90 185 598 000
		Неправомерная модификация счетов		5 404 457 000
		Неправомерное оформление кредитов		109 037 478
		Привилегированное и финансовое мошенничество	Мошенничество на руководящей должности	202 591 840 000
	Шантаж	Шантаж руководства нарушением ИБ	Нет	16 380 000
	Продажа ИОД	Продажа ИОД	Мошенничество на не руководящей должности	124 295 000

Выводы

В статье проведен анализ существующих классификаций внутренних угроз и нарушителей ИБ, отмечены их достоинства и недостатки. Выделены критерии классификации внутренних угроз ИБ. Разработан формат базы внутренних инцидентов ИБ,

сформирована база из 500 инцидентов ИБ. По выделенным критериям классификации инциденты разбиты по реализованным угрозам, угрозы переведены в векторный вид и поданы на вход алгоритмов кластеризации. Разработаны критерии оценки результатов работы алгоритмов кластеризации и проведено их сравнение. В результате получена классификация внутренних угроз ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Руководящий документ Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
2. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А. Биячуев – СПб: СПб ГУ ИТМО, 2004. – 161 с.
3. Скиба, В.Ю. Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.А. Курбатов. – СПб: Питер, 2008. – 320 с.
4. Silowash, G. Common Sense Guide to Mitigating Insider Treats 4th Edition / G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T.J. Shimeall, L. Flynn // Carnegie-Mellon University. Software Engineering Institute. CERT Program. – Pittsburg., 2012. – 144 с.
5. Cummings, A. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector / A. Cummings, T. Lewellen, D. McIntire, A.P. Moore, R. Trzeciak // Carnegie-Mellon University. Software Engineering Institute. CERT Program. – Pittsburg., 2012. – 76 с.
6. The CERT Insider Threat Team. Unintentional Insider Threats: A Foundational Study. – Carnegie-Mellon University. Software Engineering Institute, CERT Division. – Pittsburg., 2013. – 91 с.
7. IBM SPSS Modeler 16 Algorithms Guide – 2013 [Электронный ресурс] Режим доступа: ftp://public.dhe.ibm.com/software/analytics/spss/documentation/modeler/16.0/en/ AlgorithmsGuide.pdf (дата обращения 28.01.2016).

REFERENCES:

1. Rukovodyaschy document Gosudarstvennoi tehnicheskoi comissii pri Prezidente Rossiiskoi Federacii ot 30 marta 1992 g. «Concepcia zatschity sredstv vychislitelnoi tehniki I avtomatizirovannyh system ot nesankcionirovannogo dostypa k informacii».
2. Biyachuev, T.A. Bezopasnost corporativnyh setei / T.A. Biyachuev – SPb: SPb GU ITMO, 2004. – 161 p.
3. Skiba, V.Y. Rukovodstvo po zatschite ot vnutrennih ugroz informatsionnoi bezopasnosti / V.Y. Skiba, V.A. Kurbatov. – SPb: Piter, 2008. – 320 p.
4. Silowash, G. Common Sense Guide to Mitigating Insider Treats 4th Edition / G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T.J. Shimeall, L. Flynn // Carnegie-Mellon University. Software Engineering Institute. CERT Program. – Pittsburg., 2012. – 144 с.
5. Cummings, A. Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector / A. Cummings, T. Lewellen, D. McIntire, A.P. Moore, R. Trzeciak // Carnegie-Mellon University. Software Engineering Institute. CERT Program. – Pittsburg., 2012. – 76 с.
6. The CERT Insider Threat Team. Unintentional Insider Threats: A Foundational Study. – Carnegie-Mellon University. Software Engineering Institute, CERT Division. – Pittsburg., 2013. – 91 с.
7. IBM SPSS Modeler 16 Algorithms Guide – 2013 [Web resource] URL: ftp://public.dhe.ibm.com/software/analytics/spss/documentation/modeler/16.0/en/ AlgorithmsGuide.pdf (access date 28.01.2016).