ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 51-74

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ ДИНАМИЧЕСКОЙ СРЕДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛЕВКИН И.М.,
ГАЛКОВА Е.А.,

АННОТАЦИЯ

В данной работе рассматриваются множественные согласованные по целям, задачам, месту и времени формирования угрозы типа дестабилизирующего концентрированного воздействия и дестабилизирующей операции, отмечаются особенности процесса формирования угроз и построение системы информационной безопасности объекта, носящей комплексный и динамический характер. В статье дано математическое описание динамической среды угроз информационной безопасности, приведены статические и динамические параметры, описаны их информационные признаки.

Ключевые слова: угрозы безопасности; дестабилизирующее концентрированное воздействие; информационные угрозы; информационная безопасность; динамическая среда угроз; информационный признак; информационно-признаковая модель.

MATHEMATICAL DESCRIPTION OF THE DYNAMIC COMBINATION OF INFORMATION SECURITY THREATS

LEVKIN I.M.,
GALKOVA E.A.,

ABSTRACT

In this work are discussed: plural coordinated by goals, tasks, time and place of formation of threats like the destabilizing concentrated effect and the destabilizing operations; are noted features of formation process of threats and a creation of system of information security of the object, having complex and dynamic nature. In the article a mathematical description of the dynamic environment of threats to information security static and dynamic parameters and their informational attributes is given.

Keywords: threats of security; a destabilizing concentrated effect; information threats; information security; dynamic combination of threats; information attribute; informatively attributive model.

Среди множества угроз безопасности (национальной, экономической и т.п.) наиболее сложными и опасными являются множественные согласованные по целям, задачам, месту и времени формирования угрозы типа дестабилизирующего концентрированного воздействия и дестабилизирующей операции [1]. Это связано с тем, что:

– во-первых, эти угрозы являются комплексными, т.е. носят разнородный характер (внутренний, внешний, криминальный, юридический, информационный и т.д.); это требует соответствующих комплексных действий по их преодолению;

– во-вторых, интенсивность этих угроз может существенно меняться в зависимости от способа (порядка) реализации замысла достижения конечной цели структурами, реализующими угрозу; это требует оперативного перераспределения сил и средств защиты на каждом этапе противодействия комплексной угрозе;

– в-третьих, они реализуются на общем фоне традиционно существующих угроз безо-

пасности, для противодействия которым в полном объеме задействованы соответствующие силы и средства защиты.

Одной из важнейших особенностей процесса формирования любой угрозы является необходимость его информационного обеспечения. Это предполагает получение соответствующей информации об объекте, в отношении которого формируется и реализуется угроза. Таким образом, угроза безопасности любого рода сопровождается комплексом информационных угроз.

Система информационной безопасности объекта в рассматриваемом случае также должна носить комплексный и динамический характер. В основе построения такой системы должно лежать представление о мощности поля (среды) информационных угроз, их номенклатуре и динамике изменения их интенсивности. Такое представление может быть получено путем построения модели динамической среды угроз информационной безопасности.

Под динамической средой угроз информационной безопасности (ДСУ ИБ) объекта будем понимать составную часть внешней и внутренней среды функционирования объекта состоящую из разнородных информационных угроз, постоянно переходящих из потенциального состояния в реальное и обратно.

Процесс преобразования потенциальных угроз в реальные будет определяться их жизненным циклом, схема которого представлена на рисунке 1 [2].

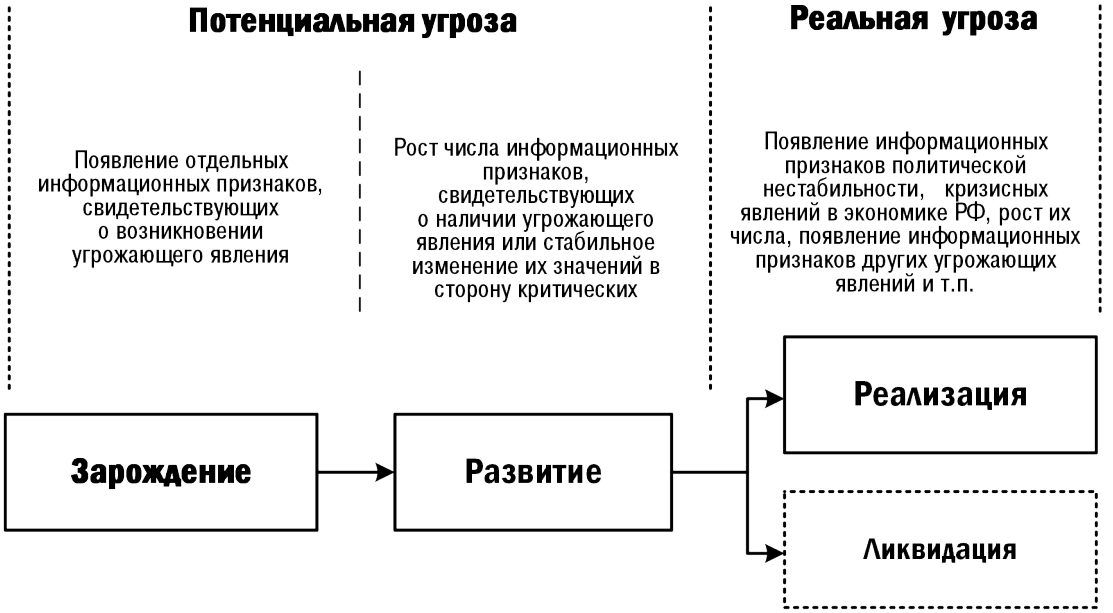

Рисунок 1 – Жизненный цикл экономической угрозы

Интенсивность преобразования потенциальных информационных угроз в реальные и их реализация будут зависеть от замысла и способа осуществления дестабилизирующих воздействий, которые могут описываться рядом параметров – моделью ДСУ ИБ.

Формализованное описание ДСУ ИБ (в канонической форме) представим в виде многомерного вектора $W_{<x>}$, включающего статистические $W^{c}_{<x'>}$ и динамические $W^{\partial}_{<x''>}$ параметры:

$$W_{<x>} = < W^{(1)}_{<\ell_1>}, \ldots, W^{(x)}_{<\ell_x>}, \ldots, W^{(X)}_{<\ell_X>} >,$$

$W^{(x)}_{<\ell_x>}$ – ℓ_x-мерный вектор параметров описывающий x-параметр ДСУ ИБ; $x = \overline{1, X}$.

$$W_{<x>} = W^{c}_{<x'>} + W^{\partial}_{<x''>}, \; x = x' + x''.$$

Каждый параметр вектора $W_{<x>}$ имеет свой информационный аналог, состоящий из одной или нескольких информационных структур (угроз), описываемых информационными признаками (информационно-признаковыми моделями).

К основным статическим параметрам относятся:

$$W^{c}_{<x'>} = W^{c}_{<6>} = < W^{c(1)}_{<\ell_1>}, W^{c(2)}_{<\ell_2>}, \ldots, W^{c(6)}_{<\ell_6>} >,$$

где:

1. $W^{c(1)}_{<\ell_1>} = W^{c(1)}_{<4>} < \omega^{c(1)}_1, \omega^{c(1)}_2, \omega^{c(1)}_3, \omega^{c(1)}_4 >$ – характер дестабилизирующего воздействия:

$\omega^{c(1)}_1$ – единичная угроза;

$\omega^{c(1)}_2$ – множественная угроза;

$\omega^{c(1)}_3$ – концентрированное дестабилизирующее воздействие;

$\omega^{c(1)}_4$ – дестабилизирующая операция.

2. $W^{c(2)}_{<\ell_2>} = W^{c(2)}_{<10>} < \omega^{c(2)}_1, \omega^{c(2)}_2, ..., \omega^{c(2)}_{10} >$ – основные причины возникновения дестабилизирующего воздействия (как внутри объекта, так и вне его):

$\omega^{c(2)}_1$ – случайное единичное внешнее воздействие (заражение вирусом, отключение питания, бросок напряжения и т.п.);

$\omega^{c(2)}_2$ – случайное единичное внутреннее воздействие (отказы и сбои в работе отдельных компьютеров, ошибки в работе их программного обеспечения, ошибки отдельных пользователей и системных администраторов, нарушения отдельными сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации и т.п.);

$\omega^{c(2)}_3$ – случайное групповое внешнее воздействие (заражение разнообразными вирусами ряда компьютеров, приобретение и использование нелицензионного программного обеспечения и т.п.);

$\omega^{c(2)}_4$ – случайное групповое внутреннее воздействие (отказы и сбои в работе ряда компьютеров, ошибки в работе их программного обеспечения, многочисленные ошибки пользователей и системных администраторов, нарушения многими сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации и т.п.);

$\omega^{c(2)}_5$ – целенаправленное враждебное действие бывших сотрудников;

$\omega^{c(2)}_6$ – целенаправленное вредительское действие сотрудников;

$\omega^{c(2)}_7$ – некачественный менеджмент на объекте;

$\omega^{c(2)}_8$ – деятельность конкурентов по получению экономических (финансовых, технологических и т.п.) преимуществ;

$\omega^{c(2)}_9$ – дискредитация объекта;

$\omega^{c(2)}_{10}$ – попытка криминальных структур захватить объект.

3. $W^{c(3)}_{<\ell_3>} = W^{c(3)}_{<7>} =< \omega^{c(3)}_1, \omega^{c(3)}_2, ..., \omega^{c(3)}_7 >$ – характер объекта:

$\omega^{c(3)}_1$ – государственный деятель;

$\omega^{c(3)}_2$ – общественный деятель;

$\omega^{c(3)}_3$ – предприятие, имеющее стратегическое значение;

$\omega^{c(3)}_4$ – государственное предприятие;

$\omega^{c(3)}_5$ – частное предприятие;

$\omega^{c(3)}_6$ – общественная организация;

$\omega^{c(3)}_7$ – объект муниципальной собственности.

4. $W^{c(4)}_{<\ell_4>} = W^{c(4)}_{<3>} =< \omega^{c(4)}_1, \omega^{c(4)}_2, \omega^{c(4)}_3 >$ – наличие на объекте сил и средств защиты информации:

$\omega^{c(4)}_1$ – в достаточном объеме;

$\omega^{c(4)}_2$ – в ограниченном объеме;

$\omega^{c(4)}_3$ – отсутствуют.

5. $W^{c(5)}_{<\ell_5>} = W^{c(5)}_{<2>} =< \omega^{c(5)}_1, \omega^{c(5)}_2 >$ – правовая база:

$\omega^{c(5)}_1$ – развита;

$\omega^{c(5)}_2$ – неразвита.

6. $W^{c(6)}_{<l_6>} = W^{c(6)}_{<3>} =< \omega^{c(6)}_1, \omega^{c(6)}_2, \omega^{c(6)}_3 >$ – напряженность внутренней обстановки:

$\omega^{c(6)}_1$ – высокая;

$\omega^{c(6)}_2$ – средняя;

$\omega^{c(6)}_3$ – низкая.

7. $W^{c(7)}_{<l_7>} = W^{c(7)}_{<3>} =< \omega^{c(7)}_1, \omega^{c(7)}_2, \omega^{c(7)}_3 >$ – напряженность внешней обстановки:

$\omega^{c(7)}_1$ – высокая;

$\omega^{c(7)}_2$ – средняя;

$\omega^{c(7)}_3$ – низкая.

К основным динамическим параметрам относятся:

$W^{\partial}_{<x''>} = W^{\partial}_{<5>} =< W^{\partial(1)}_{<h_1>}, W^{\partial(2)}_{<h_2>}, ..., W^{\partial(5)}_{<h_5>} >$, где:

1. $W^{\partial(1)}_{<h_1>} = W^{\partial(1)}_{<3>} =< \omega^{\partial(1)}_1, \omega^{\partial(1)}_2, \omega^{\partial(1)}_3 >$ – темп развития внутренней угрозы:

$\omega^{\partial(1)}_1$ – высокий;

$\omega_2^{\partial(2)}$ – средний;

$\omega_3^{\partial(3)}$ – низкий.

2. $W_{<h_2>}^{\partial(2)} = W_{<3>}^{\partial(2)} =< \omega_1^{\partial(2)}, \omega_2^{\partial(2)}, \omega_3^{\partial(2)} >$ – темп развития внешней угрозы:

$\omega_1^{\partial(2)}$ – высокий;

$\omega_2^{\partial(2)}$ – средний;

$\omega_3^{\partial(2)}$ – низкий.

3. $W_{<h_3>}^{\partial(3)} = W_{<3>}^{\partial(3)} =< \omega_1^{\partial(3)}, \omega_2^{\partial(3)}, ..., \omega_7^{\partial(3)} >$ – этапы (фазы) развития угрозы:

$\omega_1^{\partial(3)}$ – зарождение угрозы (принятие решения на формирование угрозы);

$\omega_2^{\partial(3)}$ – формирование условий для возникновения угрозы;

$\omega_3^{\partial(3)}$ – сбор информации об объекте из открытых источников;

$\omega_4^{\partial(3)}$ – проникновение в информационную структуру объекта;

$\omega_5^{\partial(3)}$ – использование законных (белых) методов (схем) реализации угрозы;

$\omega_6^{\partial(3)}$ – использование серых методов (схем) реализации угрозы;

$\omega_7^{\partial(3)}$ – использование черных методов (схем) реализации угрозы.

4. $W_{<h_4>}^{\partial(4)} =< \omega_1^{\partial(4)}, \omega_2^{\partial(4)}, \omega_3^{\partial(4)} >$ – преследуемые цели:

$\omega_1^{\partial(4)}$ – уничтожение объекта;

$\omega_2^{\partial(4)}$ – захват объекта;

$\omega_3^{\partial(4)}$ – изменение направления деятельности объекта.

5. $W_{<h_5>}^{\partial(5)} = W_{<1>}^{\partial(5)} =< \omega_1^{\partial(5)}, \omega_2^{\partial(5)}, \omega_3^{\partial(5)}, \omega_4^{\partial(5)} >$ – состав и возможности сил, формирующих угрозу:

$\omega_1^{\partial(5)}$ – отдельное лицо;

$\omega_2^{\partial(5)}$ – легальная группа лиц;

$\omega_3^{\partial(5)}$ – легальная организация;

$\omega_4^{\partial(5)}$ – криминальная группировка.

Информационные аналоги (информационные признаки) рассмотренных параметров приведены в таблице 1.

Таблица 1

Информационные аналоги параметров динамической среды угроз информационной безопасности.

Обозначение параметра	*Информационный аналог (информационный признак)*
$\omega_1^{c(1)}$	сбой работы программного обеспечения компьютера (компьютер не выполняет команды, выполняет команды неправильно и т.п.); неожиданное/неплановое выключение компьютера; поломка компьютера; признаки несанкционированного доступа к отдельным информационным базам; появление отдельных посторонних лиц вблизи информационных хранилищ (узлов); непрофессиональные действия отдельных сотрудников и т.п.
$\omega_2^{c(1)}$	сбой работы программного обеспечения нескольких компьютеров; неожиданное/неплановое выключение нескольких (или всех) компьютеров; поломка нескольких компьютеров; признаки несанкционированного доступа к информационным базам; постоянное появление посторонних лиц вблизи информационных хранилищ (узлов) и т.п.
$\omega_3^{c(1)}$	совокупность информационных признаков единичных и множественных угроз на кратковременном интервале; наличие логической связи между информационными признаками множественных угроз; информационные признаки активных действий конкурирующих организаций/лиц и т.д.
$\omega_4^{c(1)}$	совокупность информационных признаков, характерных для взаимосвязанных концентрированных дестабилизирующих воздействий; наличие логической связи между информационными признаками концентрированных дестабилизирующих воздействий; информационные признаки участия в формировании угрозы множества официальных и неофициальных (в том числе и криминальных) структур и т.д.
$\omega_1^{c(2)}$	внезапный сбой работы программного обеспечения компьютера (компьютер не выполняет команды, выполняет команды неправильно и т.п.); случайное выключение компьютера; неожиданная поломка компьютера и т.п.

Обозначение параметра	*Информационный аналог (информационный признак)*
$\omega_2^{c(2)}$	внезапный сбой работы программного обеспечения компьютера; случайное выключение компьютера; неожиданная поломка компьютера; непреднамеренное устное разглашение конфиденциальной информации; утеря конфиденциальных документов; работа за клавиатурой постороннего лица и т.п.
$\omega_3^{c(2)}$	внезапный сбой работы программного обеспечения нескольких компьютеров (компьютеры по-разному не выполняют команды, выполняют команды неправильно и т.п.); случайное выключение нескольких компьютеров; неожиданная поломка нескольких компьютеров и т.п.
$\omega_4^{c(2)}$	внезапный сбой работы программного обеспечения нескольких компьютеров; случайное выключение нескольких компьютеров; неожиданная поломка нескольких компьютеров; непреднамеренное устное разглашение различных видов конфиденциальной информации; утеря различных конфиденциальных документов; работа за клавиатурой посторонних лиц и т.п.
$\omega_5^{c(2)}$	недружественные официальные/неофициальные заявления в адрес организации (фирмы) бывших (обиженных) сотрудников; попытки несанкционированного прохода этих сотрудников на территорию организации (фирмы): их несанкционированное появление на территории организации (фирмы); активные попытки этих сотрудников вступить в контакт с действующими сотрудниками фирмы и т.п.
$\omega_6^{c(2)}$	попытки сотрудников получить доступ к конфиденциальной информации; изучение посторонними лицами системы информационной безопасности организации (фирмы); попытки сотрудников организовать протестные настроения в организации (фирме); принятие заведомо неправильных решений в интересах внешних структур; активные попытки сотрудников вступить в контакт с внешними (конкурирующими, криминальными и т.п.) структурами и т.п.
$\omega_7^{c(2)}$	принятие непрофессиональных решений; кадровая «чехарда»; нецелевое использование финансов; закупка нелицензионных продуктов и т.п.
$\omega_8^{c(2)}$	попытки несанкционированного доступа к информационным ресурсам организации (фирмы) с целью изучения технологических процессов, «ноу-хау» и т.п.; опережение в распространении информации об аналогичной продукции; изучение ценовой политики организации (фирмы), ее рекламной продукции и т.п.
$\omega_9^{c(2)}$	распространение ложных, неточных или искажённых сведений, способных причинить убытки организации либо нанести ущерб ее деловой репутации; введение потребителей в заблуждение относительно характера, способа и места изготовления, потребительских свойств, качества товара; некорректное сравнение производимых или реализуемых организацией (фирмой) товаров с товарами других хозяйствующих субъектов; продажа товара с незаконным использованием результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации юридического лица, индивидуализации продукции, выполнения работ, услуг; получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе коммерческой тайны, без согласия ее владельца и.п.
$\omega_{10}^{c(2)}$	попытки несанкционированного доступа к юридическим, экономическим и т.п. документам организации; внедрение на руководящие и ключевые посты организации агентов влияния; вербовка сотрудников из системы управления организации; резкий рост частоты проверок деятельности организации со стороны налоговых, надзорных и других органов; оспаривание прав собственности; изучение посторонними лицами системы информационной безопасности организации и т.п.
$\omega_1^{c(3)}$	изучение особенностей характера государственного деятеля (руководителя организации), пристрастий, предпочтений путем опроса его коллег, друзей, знакомых и т.п.; появление в его окружении подозрительных лиц; попытки шантажа, т.п.
$\omega_2^{c(3)}$	изучение особенностей характера общественного деятеля, пристрастий, предпочтений путем опроса его коллег, друзей, знакомых и т.п.; появление в его окружении подозрительных лиц; попытки шантажа и т.п.

Обозначение параметра	*Информационный аналог (информационный признак)*
$\omega_3^{c(3)}$	попытки несанкционированного доступа к юридическим, экономическим и т.п. документам организации; внедрение на руководящие и ключевые посты организации агентов влияния; вербовка сотрудников из системы управления организации; изучение посторонними лицами системы информационной безопасности организации; лоббирование интересов конкурирующей (враждебной) стороны в федеральных органах власти; попытки включения предприятия в более крупную структуру и т.п.
$\omega_4^{c(3)}$	попытки несанкционированного доступа к юридическим, экономическим и т.п. документам организации; внедрение на руководящие и ключевые посты организации агентов влияния; вербовка сотрудников из системы управления организации; изучение посторонними лицами системы информационной безопасности организации; лоббирование интересов конкурирующей (враждебной) стороны в государственных органах власти; попытки акционирования предприятия и т.п.
$\omega_5^{c(3)}$	попытки несанкционированного доступа к юридическим, экономическим и т.п. документам организации; внедрение на руководящие и ключевые посты организации агентов влияния; вербовка сотрудников из системы управления организации; изучение посторонними лицами системы информационной безопасности организации; попытки рейдерского захвата организации и т.п.
$\omega_6^{c(3)}$	попытки смены лидера общественной организации; попытки изменить направления общественной деятельности; дискредитация деятельности общественной организации и ее влиятельных членов; изучение посторонними лицами системы информационной безопасности общественной организации и т.п.
$\omega_7^{c(3)}$	попытки несанкционированного доступа к юридическим, экономическим и т.п. документам муниципального объекта; внедрение на руководящие и ключевые посты муниципального объекта агентов влияния; вербовка сотрудников из системы управления муниципального объекта; изучение посторонними лицами системы информационной безопасности муниципального объекта; лоббирование интересов конкурирующей (враждебной) стороны в высших органах власти; попытки рейдерского захвата организации и т.п.
$\omega_1^{c(4)}$	наличие современных средств защиты информации; наличие квалифицированных специалистов по защите информации; крайне редкие случаи нарушения информационной безопасности и т.п.
$\omega_2^{c(4)}$	частичное наличие современных средств защиты информации; наличие отдельных квалифицированных специалистов по защите информации; частые случаи нарушения информационной безопасности и т.п.
$\omega_3^{c(4)}$	наличие несовершенных или устаревших средств защиты информации; отсутствие квалифицированных специалистов по защите информации; постоянные случаи нарушения информационной безопасности и т.п.
$\omega_1^{c(5)}$	наличие полного комплекта документов, регламентирующих информационную безопасность организации (фирмы); наличие квалифицированных юристов в штате организации (фирмы) и т.п.
$\omega_2^{c(5)}$	ограниченное число документов, регламентирующих информационную безопасность организации; наличие устаревших документов, регламентирующих информационную безопасность организации; отсутствие квалифицированных юристов в штате организации и т.п.
$\omega_1^{c(6)}$	постоянные конфликты сотрудников организации между собой; постоянные конфликты сотрудников с руководством организации; кадровая «чехарда» в организации; отсутствие службы психологической поддержки и т.п.
$\omega_2^{c(6)}$	наличие конфликтов сотрудников организации между собой; наличие конфликтов сотрудников с руководством организации; успешные случаи взаимного улаживания конфликтов и т.п.
$\omega_3^{c(6)}$	редкие конфликты сотрудников организации между собой (отсутствие конфликтов); отсутствие конфликтов сотрудников с руководством организации; наличие службы психологической поддержки и т.п.

Обозначение параметра	*Информационный аналог (информационный признак)*
$\omega_1^{c(7)}$	частые недружественные действия в отношении организации и ее представителей; высокий уровень криминализации общества; высокий уровень коррупции чиновников региона (страны); отсутствие развитой нормативно-правовой базы в сфере информационной безопасности и т.п.
$\omega_2^{c(7)}$	наличие недружественных действий в отношении организации и ее представителей; средний уровень криминализации общества; наличие фактов коррупции чиновников региона (страны); наличие нормативно-правовых документов в сфере информационной безопасности и т.п.
$\omega_3^{c(7)}$	отсутствие недружественных действий в отношении организации и ее представителей; низкий уровень криминализации общества; редкие факты коррупции чиновников региона; наличие развитой нормативно-правовой базы в сфере информационной безопасности и т.п.
$\omega_1^{\partial(1)}$	частое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_2^{\partial(1)}$	периодическое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_3^{\partial(1)}$	редкое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_1^{\partial(2)}$	частое проявление информационных признаков внешних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_2^{\partial(2)}$	периодическое проявление информационных признаков внешних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_3^{\partial(2)}$	редкое проявление информационных признаков внешних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_1^{\partial(3)}$	повышение активности отдельных сотрудников (акционеров) организации во внешней (конкурентной, криминальной и т.п.) среде; попытка расширить (изменить) состав органов управления организации; неожиданные изменения в составе акционеров, руководства; нестандартное поведение отдельных (как правило, миноритарных) акционеров; проявление заинтересованности посторонних (третьих) лиц организационным, финансовым, экономическим и т.п. состоянием организации и т.п.
$\omega_2^{\partial(3)}$	информационные признаки характера дестабилизирующего воздействия, причин их возникновения, низкого состояния защиты информации, высокой напряженности внешней и внутренней обстановки; появление заинтересованности третьих лиц и/или структур в изменении судьбы организации и т.п.
$\omega_3^{\partial(3)}$	активное посещение сайта организации конкурентами, подозрительными лицами и т.п.; тщательное изучение ими рекламных материалов организации; повышенная активность третьих лиц при общении с сотрудниками организации на официальных мероприятиях (выставках, конференциях и т.п.) и т.п.
$\omega_4^{\partial(3)}$	попытки несанкционированного доступа к информационным ресурсам организации со стороны сторонних пользователей, связанных с конкурирующими, криминальными и т.п. структурами; попытки несанкционированного доступа к информационным ресурсам организации со стороны внутренних пользователей; попытки несанкционированного доступа к реестру владельцев акций кредитно-финансового учреждения и т.п.
$\omega_5^{\partial(3)}$	постоянные требования гринмеэйлеров предоставления большого объема информации и документов компании, включая финансовую отчетность; подача ими многочисленных жалоб в госорганы надзора; бесконечное предъявление исков, часто не обоснованных и т.п.
$\omega_6^{\partial(3)}$	появление судебных актов, постановлений судебных приставов-исполнителей, арестов акций и имущества, запретов органам управления принимать определенные решения и т.п.

Обозначение параметра	*Информационный аналог (информационный признак)*
$\omega_7^{\partial(3)}$	информационные признаки угроз, шантажа, фальсификации документов и т.п.
$\omega_1^{\partial(4)}$	заявления о необходимости использования территории, занимаемой объектом в других целях; информационное воздействие на общественное мнение о необходимости ликвидации организации и т.п.
$\omega_2^{\partial(4)}$	попытки подделки документов регистрации организации, формирования подконтрольных рейдерам органов управления, назначения нового генерального директора и т.д.
$\omega_3^{\partial(4)}$	введение в руководство организации специалистов другого профиля; закупка средств производства не соответствующего профилю организации; переподготовка кадров в новом направлении и т.п.
$\omega_1^{\partial(5)}$	информационные признаки конкретного лица и осуществляемых им действий
$\omega_2^{\partial(5)}$	информационные признаки отдельных лиц, признаки наличия у них общих интересов и осуществляемых ими действий
$\omega_3^{\partial(5)}$	информационные признаки организации и осуществляемых ею действий
$\omega_4^{\partial(5)}$	информационные признаки криминальной группировки и осуществляемых ею действий

Основной особенностью предлагаемой модели является то, что многие информационные признаки могут принадлежать различным по своей природе угрозам. Это предполагает целенаправленный поиск дополнительных информационных признаков для более точной идентификации угрозы.

Предложенная модель позволяет:

- во-первых, по совокупности зафиксированных информационных признаков определить наличие и состояние угроз безопасности в целом, и информационных угроз, в частности;
- во-вторых, построить информационно-признаковые модели информационных угроз;
- в-третьих, определить интенсивность информационных угроз и и динамику ее изменения;
- в-четвертых, сформировать исходные данные для построения оптимальной системы информационной безопасности.

Список литературы

1. Левкин И. М., Левкина С. В., Сорокина Е. А. Информационно-признаковое моделирование угроз национальной безопасности // Вестник Академии военных наук. Северо-Западное отделение. – 2013.

2. Левкина С. В. Модели угроз экономической безопасности // XVI Всероссийская научно-практическая конференция «Актуальные вопросы защиты и безопасности» 3-6 апреля 2013, СПб: РАРАН. – 2013.