УДК 004.056

Галкова Елена Александровна
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
Россия, Санкт-Петербург[1]
Аспирант
sorokina_elena_@mail.ru

Информационно-признаковая модель угроз безопасности организации

Аннотация. Целью данной работы было построение информационно-признаковой модели угроз безопасности организации. В ходе исследования были рассмотрены: особенности информационно-признакового моделирования угроз безопасности организации, затронут вопрос формирования информационной базы обеспечения безопасности функционирования объекта (процесса). Представлена структура угрозы, описаны особенности предложенной структуры угрозы. Предложена методика разработки информационного портрета угроз. В ходе работы разработаны и представлены: обобщенная информационно-признаковая модель статической угрозы предприятию (организации), обобщенная информационно-признаковая модель совокупности угроз, агрегированная пространственно-временная модель рейдерского захвата, информационно-признаковая модель (в терминах мероприятий) рейдерского захвата организации. Предложен математический аппарат, использованный для численной оценки вероятности возникновения и развития угроз по совокупности проявившихся информационных признаков. Сделаны выводы о том, что построение информационно-признаковых моделей (информационных портретов) угроз предприятию (организации) позволяют: осуществлять мониторинг внешней и внутренней среды функционирования предприятия (организации) путем сканирования информационного пространства с целью выявления информационных признаков угроз; формировать исходные данные для текущего распределения сил и средств защиты информации, лежащей в основе формирования большинства угроз; прогнозировать наступление угроз предприятию (организации) на ближайшую перспективу.

Ключевые слова: информационное обеспечение безопасности; информационно-признаковая модель; информационная угроза; структура угрозы; информационный портрет угроз; статическая угроза организации; обобщенная пространственно-временная модель; рейдерский захват; защита информации, распределение сил и средств защиты информации.

[1] 197371, Санкт-Петербург, ул. Шаврова, д. 23, корп. 1, кВ. 89

С развитием информационного общества возникает понимание того, что информация становится стратегической субстанцией, которая может либо непосредственно, либо косвенно (например, в форме информационного обеспечения) как созидать, так и разрушать.

Одним из характерных признаков такого информационного общества является понимание того, что эффективность протекания любых целенаправленных процессов в определяющей степени зависит от качества их информационного обеспечения. Важнейшими элементами информационного обеспечения является:

- формирование благоприятной информационной среды;
- формирование системы защиты информационной среды.

Формирование благоприятной информационной среды в свою очередь может включать в себя следующие основные компоненты:

- информационную базу предметной области, в объеме необходимом для успешного достижения цели функционирования объекта (процесса);
- информационную базу обеспечения безопасности функционирования объекта (процесса).

Из перечисленных элементов информационного обеспечения особое значение имеет компонента, связанная с формированием информационной базы обеспечения безопасности функционирования объекта (процесса). Это связано с тем, что:

- во-первых, безопасность является одним из важнейших необходимых условий функционирования любого объекта (процесса) и ее обеспечение зависит от знания информационных характеристик угроз;
- во-вторых, угрозы объекту (процессу) имеют ярко выраженный след в информационном пространстве в виде информационных (идентификационных) признаков и могут быть выявлены на ранних стадиях;
- в-третьих, именно информационные портреты большинства угроз могут и должны составлять основу формирования системы защиты информации.

Вместе с тем вопросы формирования информационной базы обеспечения безопасности функционирования объекта (процесса) в системном плане, как правило, не рассматриваются. В лучшем случае они косвенно обозначаются как сопутствующий элемент системы защиты информации.

В основу информационного обеспечения безопасности процесса функционирования объекта (процесса) должны быть положены информационно-признаковые (информационные, идентификационные) модели внутренних и внешних угроз. В общем виде под информационно-признаковыми моделями понимают каким-либо образом упорядоченную совокупность сведений о связях показателей функционирования объектов (процессов) наблюдения, их информационных (идентификационных) признаков и признаков проводимых мероприятий с состояниями объекта (процессов) наблюдения. В свою очередь под информационными (идентификационными) признаками объектов (процессов) наблюдения понимают физические поля и отдельные свойства объектов (явлений) наблюдения, их частные характеристики, действия (мероприятия), изменения в среде действий и обстоятельства деятельности объектов, частные элементы обстановки, причинно-следственные и сопутствующие явления.

Для построения таких моделей сначала необходимо уточнить понятие угрозы, так как единого общепризнанного научно разработанного подхода к этому явлению не существует.

Соответственно отсутствует научно обоснованный механизм моделирования процесса формирования угроз. Опираясь на выводы работ Гацко М. и Жигулина Г.П., представим структуру угрозы любой природы так, как показано на рисунке 1.

Рис. 1. *Структура угрозы*

(Lean Manufacturing)

Особенностями данного представления угрозы являются следующие.

1. Разделение необходимых и достаточных условий для формирования объективной возможности субъективных намерений на условия, создаваемые субъектом и условия, складывающиеся без участия субъекта.

Условия, создаваемые субъектом, представляют собой результат целенаправленной деятельности по потенциальному нарушению процесса функционирования предприятия (организации). К таким условиям могут быть отнесены: несанкционированное обладание субъектом конфиденциальной информацией; формирование дополнительных юридических, экономических, финансовых и т.п. сложностей и препятствий во внешней и внутренней среде; криминализация обстановки и т.п.

Условия, складывающиеся без участия субъекта, в данном случае, рассматриваются как внутренние. К ним можно отнести: некачественный менеджмент предприятия (организации); низкую производственную дисциплину; высокую текучесть кадров и т.п.

2. Установление взаимосвязи между субъективными намерениями (замыслами (желаниями)) с наличием у субъекта соответствующих сил и средств и формированием условий для реализации субъективных намерений.
3. Учет объективно сложившихся неблагоприятных условий и факторов, которые могут быть использованы субъектом для нанесения ущерба предприятию (организации). Эти условия являются внешними, как правило, никак не связанные с конкретными предприятиями (организациями). Примерами таких условий являются: кризисные явления в экономике, возникновение нестабильностей и горячих точек в отдельных регионах мира, и т.п.

При разработке информационных портретов угроз предприятию (организации) следует выделять их статическую и динамическую природу.

Под статической информационно-признаковой моделью угрозы будем понимать сложившуюся на конкретный момент времени совокупность информационных признаков и связей между ними.

Под динамической информационно-признаковой моделью угрозы будем понимать процесс формирования субъектом совокупности неблагоприятных условий для функционирования предприятия (организации).

В таком случае информационный портрет угрозы предприятию (организации) будет представлять собой совокупность статических и динамических информационно-признаковых моделей.

Кроме того, в процессе моделирования следует учитывать иерархию информационных признаков и их связь с иерархией угроз. Это значит, что угрозой может являться и элементарный информационный признак (например, установленная попытка получить несанкционированный доступ к конфиденциальной информации), и информационный признак-мероприятие (например, хищение конфиденциальной информации), и их совокупности.

Обобщенная информационно-признаковая модель статической угрозы представлена на рисунке 2. На нем обозначено:

a_i – i–й информационный признак U_k–й угрозы, $i=\overline{1,I}$, I– общее число информационных признаков в априорном словаре угрозы;

$P(U_k/a_1a_2..a_i)$– вероятность вскрытия U_k – й угрозы по $(a_1,a_2,..a_i)$–й совокупности информационных признаков.

В зависимости от характера информационного признака a_i вероятность вскрытия U_k – й угрозы $P(U_k/a_i)$– будет различной (рис. 2 б).

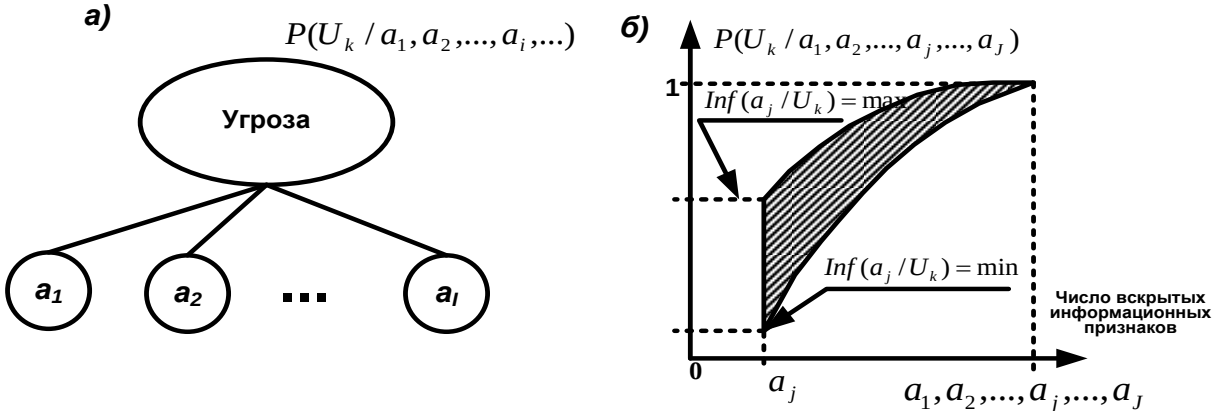


Рис. 2. *Обобщенная информационно-признаковая модель статической угрозы организации (разработано автором)*

Вероятность вскрытия U_k – й угрозы по совокупности информационных признаков $(a_1,a_2,..a_i)$ будет определяться известной формулой:

$$P(U_k/a_1a_2..a_i)=1-\prod_i(1-P(U_k/a_i))$$

В качестве примера рассмотрим статическую информационно-признаковую модель угрозы «осуществление несанкционированного доступа к конфиденциальной информации».

Основными информационными признаками этой угрозы являются:

a_1 – регистрация появления на рабочей станции искаженных данных;

a_2 – сбой либо длительное отсутствие обновления средств защиты компьютерной системы (паролей, кодов доступа и т.п.);

a_3 – регистрация увеличения количества сбоев в работе компьютерной системы и/или рабочей станции;

a_4 – регистрация увеличения количества жалоб пользователей на работу компьютерной сети и/или рабочей станции;

a_5 – нарушение внутреннего регламента подготовки/оформления документов;

a_6 – появление дополнительных (лишних) документов, подготовленных и обрабатываемых на рабочей станции ответственного сотрудника;

a_7 – нарушение установленного регламента по подготовке внутренних документов;

a_8 – подготовка нескольких лишних копий документов;

a_9 – предоставление лишних документов для обработки на рабочей станции;

a_{10} – несоответствие информации, находящейся в первичных документах, и информации, подвергнутой обработке;

a_{11} – подозрительное/преднамеренное искажение, уничтожение и/или утрата первичных источников информации, внесение недостоверных данных при регистрации полученной информации;

a_{12} – систематическое и беспричинное нарушение эксплуатации рабочей станции сотрудником;

a_{13} – использование посторонних носителей информации без предварительной проверки антивирусными программами;

a_{14} – игнорирование установленного регламента в отношении резервного копирования важных данных.

Обычно перед выше указанными информационными признакам осуществления угрозы «осуществление несанкционированного доступа к конфиденциальным данным» или параллельно с ними осуществляются следующие действия:

- осуществление незапланированных/беспричинных сверхурочных работ;
- немотивированный отказ ответственных за работу компьютерной системы/сети сотрудников от отпусков/больничных;
- появление на рабочем месте сотрудника личного компьютера (ноутбука и т.п.);
- появление на рабочем месте сотрудника личных запоминающих устройств (флешки, переносные жесткие накопители данных и т.п.);
- регистрация возрастания количества случаев перезаписи / дублирования / модификации данных без веских причин;
- появление немотивированного интереса отдельных сотрудников к служебной информации других работников.

В конечном виде модель угрозы «осуществление несанкционированного доступа к конфиденциальной информации» будет иметь вид, аналогичный рис. 2 а.

Одна из особенностей информационно-признакового моделирования угроз заключается в том, что один и тот же информационный признак может принадлежать различной по характеру угрозе. Например, установленная попытка получить несанкционированный доступ к конфиденциальной информации (информационный признак a_1 рис. 3) может принадлежать случайной, целевой единичной, целевой множественной и системной угрозам. Это вызывает определенные сложности в выявлении характера угрозы, особенно при недостатке соответствующей информации.

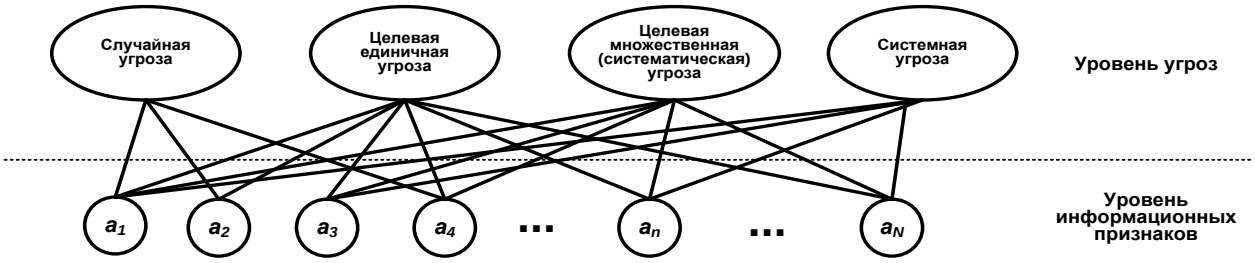


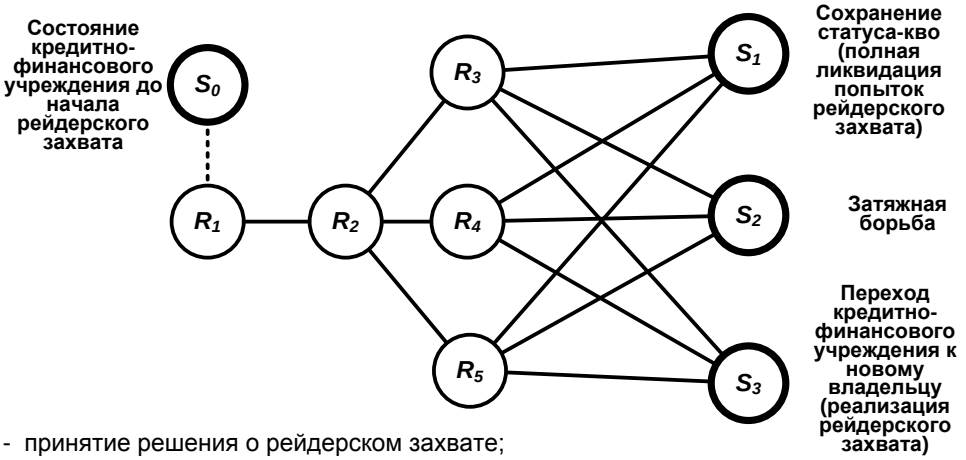
Рис. 3. *Обобщенная информационно-признаковая модель совокупности угроз*

(разработано автором)

Построение динамической информационно-признаковой модели угрозы базируется на пространственно-временной последовательности мероприятий, формирующих угрозу (неблагоприятные условия и факторы). Эта последовательность, по сути своей представляет собой информационно-признаковую модель угрозы в терминах мероприятий. В свою очередь каждое мероприятие рассматривается как статическая (или динамическая) информационно-признаковая модель структурного элемента угрозы.

В качестве примера рассмотрим построение такой системной угрозы предприятию (организации), как его рейдерский захват.

Агрегированная пространственно-временная модель рейдерского захвата рассмотрена на примере кредитно-финансового учреждения и представлена на рисунке 4.



R_1 - принятие решения о рейдерском захвате;
R_2 - сбор информации о кредитно-финансовом учреждении;
R_3 - белый рейдерский захват;
R_4 - серый рейдерский захват;
R_5 - черный рейдерский захват.

Рис. 4. *Агрегированная пространственно-временная модель рейдерского захвата (разработано автором)*

Анализ типовых вариантов осуществления рейдерских захватов предприятий (организаций) позволил выявить следующие общие мероприятия:

M_1 – повышение активности отдельных акционеров (участников) кредитно-финансового учреждения во внешней (конкурентной, криминальной и т.п.) среде;

M_2 – попытка расширить (изменить) состав органов управления кредитно-физического учреждения, неожиданные изменения в составе акционеров, руководства;

M_3 – нестандартное поведение отдельных (как правило, миноритарных) акционеров;

M_4 – проявление заинтересованности посторонних (третьих) лиц организационным, финансовым, экономическим и т.п. состоянием кредитно-финансового учреждения;

M_5 – попытки несанкционированного доступа к информационным ресурсам кредитно-финансового учреждения со стороны сторонних пользователей, связанных с конкурирующими, криминальными и т.п. структурами;

M_6 – попытки несанкционированного доступа к информационным ресурсам кредитно-финансового учреждения со стороны внутренних пользователей;

M_7 – попытки несанкционированного доступа к реестру владельцев акций кредитно-финансового учреждения;

M_8 – проведение внеплановых (неожиданных) проверок со стороны налоговых и контролирующих органов (ЦБ РФ, ФСФР, Прокуратура и пр.), приостановление нормального функционирования организации в результате проведения таких внеплановых проверок;

M_9 – участившиеся запросы акционеров о предоставлении тех или иных документов (от бухгалтерской отчетности до трудового контракта с генеральным директором);

M_{10} – подача различных исков в суд контрагентами и акционерами общества;

M_{11} – оспаривание прав собственности;

M_{12} – попытки проникновения на территорию кредитно-финансового учреждения посторонних лиц, связанных с конкурирующими, криминальными и т.п. структурами;

M_{13} – участившиеся случаи появления личных проблем у руководства и фактических владельцев бизнеса, оказание психологического давления;

регистрация фактов блокировки/задержки финансирования из внешних источников;

M_{14} – регистрация фактов блокировки/задержки финансирования из внешних источников;

M_{15} – резкое появление и увеличение случаев возбуждения судебных разбирательств и увеличения числа жалоб (в том числе надуманных, ложных) в надзорные органы в отношении руководства и фактических владельцев бизнеса;

M_{16} – участившиеся случаи появления технических проблем разного уровня в организации;

M_{17} – появление и увеличение случаев возбуждения судебных разбирательств и увеличения числа жалоб (в том числе надуманных, ложных) в надзорные органы в отношении основных поставщиков/заказчиков организации;

M_{18} – появление внутри коллектива негативных тенденций во взаимоотношениях, увольнение по собственному желанию нескольких ведущих специалистов организации, провокация коллектива атакуемой организации;

M_{19} – участившиеся случаи появления негативной информации в СМИ дестабилизирующего характера;

M_{20} – регистрация факта совершения сделок, трудно объяснимых с точки зрения бизнес-логики эффективного функционирования организации;

M_{21} – регистрация факта начала скупки кредиторской задолженности организации;

M_{22} – регистрация появления фактов обнаружения поддельной документации;

M_{23} – участившиеся случаи появления неких лиц, предлагающих финансовую или иную помощь в случае возникновения в будущем разного рода проблем.

В этом случае информационно-признаковая модель рейдерского захвата кредитно-финансового учреждения может быть представлена в виде рисунка 5.

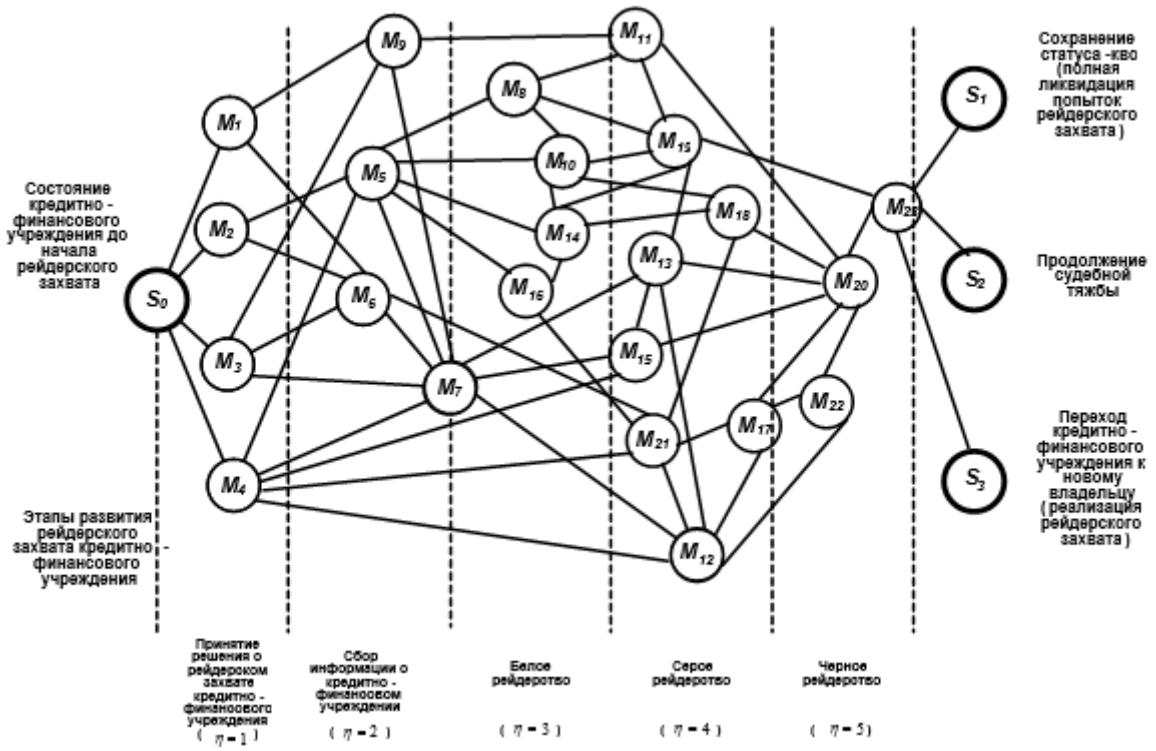


Рис. 5. *Информационно-признаковая модель (в терминах мероприятий) рейдерского захвата организации*

(разработано автором)

Построение информационно-признаковых моделей (информационных портретов) угроз предприятию (организации) позволяют:

- осуществлять мониторинг внешней и внутренней среды функционирования предприятия (организации) путем сканирования информационного пространства с целью выявления информационных признаков угроз;
- формировать исходные данные для текущего распределения сил и средств защиты информации, лежащей в основе формирования большинства угроз;
- прогнозировать наступление угроз предприятию (организации) на ближайшую перспективу.

Так же своевременное вскрытие рассмотренных условий и взаимосвязей поможет сформировать исходные данные для построения эффективной системы информационной безопасности предприятия (организации).

ЛИТЕРАТУРА

1. Гацко М. О соотношении понятий «угроза» и «опасность». [Электронный ресурс] – Режим доступа: http://old.nasledie.ru/oboz/N07_97/7_06.HTM.
2. Ефимов А.Н. Информация: ценность, старение, рассеяние. – М.: Наука, 1983.
3. Жигулин Г.П. Теория и практика прогнозирования. – СПб: СПбНИУ ИТМО, 2011.
4. Конев И., Беляев А. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.: ил.
5. Криминалистика. /Под редакцией Е.П. Ищенко [Электронный ресурс] – М.: Юристъ, 2000. – Режим доступа: http://www.bibliotekar.ru/criminalistika-1/index.htm.
6. Левкин И.М. Теория и практика информационно-аналитической работы. – Курск: НАУКОМ, 2011.
7. Левкин И.М., Левкина С.В., Сорокина Е.А. Информационно-признаковое моделирование угроз национальной безопасности//Вестник Академии военных наук. Северо-Западное отделение, 2013.
8. Левкин И.М., Сорокина Е.А. Рейдерский захват как особая форма информационно-экономической угрозы//Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции. – СПб: СПОИСУ, 2013. - Информационно-экономическая безопасность. – С. 187. – 293 с. - ISBN 978-5-906555-02-1.
9. Левкин И.М., Сорокина Е.А. Анализ возможностей получения несанкционированного доступа к информационной системе организации // Труды XVI Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности». - Санкт-Петербург, 2013.
10. Памятка гражданину из серии «Библиотечка антикоррупционера» Если Вам угрожает рейдерство. Памятка подготовлена на основании решения подкомиссии Общественной палаты Российской Федерации по проблемам противодействия коррупции от 20 июня 2006 года [Электронный ресурс] – Режим доступа: http://www.gov.karelia.ru/gov/Leader/Reform/raider.pdf.

Рецензент: Левкин Игорь Михайлович, проф., д.в.н., действительный член АВН, заведующий кафедрой Бортовых приборов управления вооружения и военной техники Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.

Elena Galkova
Federal government budgetary institution of higher professional education St. Petersburg national research university of information technologies, mechanics & optics
Russia, St. Petersburg
sorokina_elena_@mail.ru

The informationally-attributive model of a threat security organization

Abstract. The objective of the work was to construct of the informationally-attributive model of threats security organization. In the research were reviewed: details of informationally-attributive modeling of threats security organization, question about forming the information base of safety assurance of the function of the object (process). In the article was presented structure of threat, were described features of this structure of threat. Also was offered the methodical elaboration of the information portrait of threats. In the research were elaborated and shown: the generalized informationally-attributive model of static threat to a company (organization), the generalized informationally-attributive model of combination of threats, the aggregate spatial-temporary model of raider capture, the informationally-attributive model (in terms of action) of raider capture of organization. Was offered the mathematical apparatus, which used for numerical evaluation of the probability of occurrence and evolution of threats in aggregate of manifested information attributes. Were done conclusions, that the construct of informationally-attributive model (informational portraits) of threats to a company (organization) allows: to do monitor of the external and internal functional milieu of a company (organization) using a scan of information area for finding information attributes of threats; to form the basic data for the current for redistribution forces and funds of information security which situated in basis the formation of most of threats; to predict the occurrence of threats to a company (organization) on nearest perspective.

Keywords: information safety assurance; informationally-attributive model; information threat; structure of threat; information portrait of threats; static threat to a organization; aggregate spatial-temporary model; raider capture; information security; redistribution forces and funds of information security.

REFERENCES

1. Gatsko M. O sootnoshenii ponyatiy «ugroza» i «opasnost'». [Elektronnyy resurs] – Rezhim dostupa: http://old.nasledie.ru/oboz/N07_97/7_06.HTM.
2. Efimov A.N. Informatsiya: tsennost', starenie, rasseyanie. – M.: Nauka, 1983.
3. Zhigulin G.P. Teoriya i praktika prognozirovaniya. – SPb: SPbNIU ITMO, 2011.
4. Konev I., Belyaev A. Informatsionnaya bezopasnost' predpriyatiya. – SPb.: BKhV-Peterburg, 2003. – 752 s.: il.
5. Kriminalistika./Pod redaktsiey E.P. Ishchenko [Elektronnyy resurs] – M.: Yurist", 2000. – Rezhim dostupa: http://www.bibliotekar.ru/criminalistika-1/index.htm.
6. Levkin I.M. Teoriya i praktika informatsionno-analiticheskoy raboty. – Kursk: NAUKOM, 2011.
7. Levkin I.M., Levkina S.V., Sorokina E.A. Informatsionno-priznakovoe modelirovanie ugroz natsional'noy bezopasnosti//Vestnik Akademii voennykh nauk. Severo-Zapadnoe otdelenie, 2013.
8. Levkin I.M., Sorokina E.A. Reyderskiy zakhvat kak osobaya forma informatsionno-ekonomicheskoy ugrozy//Informatsionnaya bezopasnost' regionov Rossii (IBRR-2013). VIII Sankt-Peterburgskaya mezhregional'naya konferentsiya. Sankt-Peterburg, 23-25 oktyabrya 2013 g.: Materialy konferentsii. – SPb: SPOISU, 2013. - Informatsionno-ekonomicheskaya bezopasnost'. – S. 187. – 293 s. - ISBN 978-5-906555-02-1.
9. Levkin I.M., Sorokina E.A. Analiz vozmozhnostey polucheniya nesanktsionirovannogo dostupa k informatsionnoy sisteme organizatsii // Trudy XVI Vserossiyskoy nauchno-prakticheskoy konferentsii «Aktual'nye problemy zashchity i bezopasnosti». - Sankt-Peterburg, 2013.
10. Pamyatka grazhdaninu iz serii «Bibliotechka antikorruptsionera» Esli Vam ugrozhaet reyderstvo. Pamyatka podgotovlena na osnovanii resheniya podkomissii Obshchestvennoy palaty Rossiyskoy Federatsii po problemam protivodeystviya korruptsii ot 20 iyunya 2006 goda [Elektronnyy resurs] – Rezhim dostupa: http://www.gov.karelia.ru/gov/Leader/Reform/raider.pdf.