Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/
Выпуск 6 (25) 2014 ноябрь – декабрь http://naukovedenie.ru/index.php?p=issue-6-14
URL статьи: http://naukovedenie.ru/PDF/97TVN614.pdf
DOI: 10.15862/97TVN614 (http://dx.doi.org/10.15862/97TVN614)

УДК 004.056

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

Левкин Игорь Михайлович
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
Россия, Санкт-Петербург
Заведующий кафедрой Бортовых приборов управления вооружения и военной техники
Доктор военных наук, профессор, действительный член АВН
E-mail: lev.kin@yandex.ru

Модель динамической среды информационных угроз кредитно-финансового учреждения

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

Аннотация. В данной статье дается описание множественных согласованных по целям, задачам, месту и времени формирования угроз типа дестабилизирующего концентрированного воздействия. В качестве примера таких угроз приводится угроза рейдерского захвата кредитно-финансового учреждения, сопровождающаяся нарушением информационной безопасности.

Так же в статье отмечаются особенности процесса формирования угроз и построение системы информационной безопасности кредитно-финансового учреждения, носящей комплексный и динамический характер, приведено каноническое описание динамической среды угроз информационной безопасности кредитно-финансового учреждения, представлен фрагмент описания информационных признаков статических и динамических параметров разработанной модели. Сделан вывод, что предложенную модель динамической среды информационных угроз отличает целенаправленный поиск дополнительных (сопутствующих) информационных признаков для более точной идентификации угрозы. Предложенная модель позволяет: во-первых, по совокупности зафиксированных информационных признаков определить наличие и состояние угроз безопасности кредитно-финансового учреждения в целом, и информационных угроз, в частности; во-вторых, построить информационно-признаковые модели информационных угроз кредитно-финансового учреждения; в-третьих, определить интенсивность и динамику информационных угроз; в-четвертых, сформировать исходные данные для построения эффективной и оптимальной системы защиты информации кредитно-финансового учреждения.

Ключевые слова: информационная угроза; безопасность; кредитно-финансовое учреждение; динамическая угроза; динамическая среда; интенсивность угроз; информационный признак; статические параметры угрозы; динамические параметры угрозы; дестабилизирующий концентрированный эффект.

Ссылка для цитирования этой статьи:

Галкова Е.А., Левкин И.М. Модель динамической среды информационных угроз кредитно-финансового учреждения // Интернет-журнал «НАУКОВЕДЕНИЕ» 2014. № 6 http://naukovedenie.ru/PDF/97TVN614.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ. DOI: 10.15862/97TVN614

Среди множества информационных угроз безопасности кредитно-финансового учреждения наиболее сложными и опасными являются множественные согласованные по целям, задачам, месту и времени формирования угрозы типа дестабилизирующего концентрированного воздействия. Это связано с тем, что: во-первых, эти угрозы носят комплексный характер (в связи с этим требуются соответствующие комплексные действия по их преодолению); во-вторых, интенсивность угроз данного вида может существенно меняться в зависимости от выбранного сценарного подхода к достижению конечной цели агрессора (инициатора угрозы), (в связи с этим требуется оперативное перераспределение сил и средств защиты на каждом этапе противодействия комплексной угрозе); в-третьих, угрозы данного вида реализуются на общем фоне традиционно существующих угроз безопасности, для противодействия которым в полном объеме задействованы соответствующие силы и средства защиты. В итоге множественная угроза представляет собой совокупность единичных угроз одного или нескольких видов, которые могут быть согласованными или несогласованными по целям, задачам, месту и времени формирования.

В данной работе будем говорить о дестабилизирующем концентрированном воздействии на кредитно-финансовое учреждение. Под дестабилизирующим концентрированным воздействием на кредитно-финансовое учреждение в частности будем понимать совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени угроз различного вида (внутренних и внешних; технических, информационных, экономических и т.п.), сосредоточенных во времени (одновременных) и формируемых по единому плану и замыслу, которые нацелены на дискредитацию или подчинение отдельных структур кредитно-финансового учреждения – рейдерскому захвату.

Так же под дестабилизирующей операцией будем понимать совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени, разнородных единичных и массированных угроз и дестабилизирующих концентрированных воздействий, которые формируются одновременно и последовательно в соответствии с единым планом и замыслом для нанесения существенного ущерба кредитно-финансовому учреждению в установленный период времени.

Одной из важнейших особенностей процесса формирования любой угрозы является необходимость его информационного обеспечения. Это предполагает получение соответствующей информации о выбранном для реализации угрозы (атаке) объекте, в нашем случае о кредитно-финансовом учреждении. Таким образом, угроза безопасности кредитно-финансового учреждения в ходе реализации дестабилизирующего концентрированного воздействия, а именно рейдерского захвата, сопровождается комплексом информационных угроз. Рассмотрим рейдерский захват как дестабилизирующую операцию в части угрозы информационной безопасности кредитно-финансового учреждения.

Система информационной безопасности кредитно-финансового учреждения при угрозе рейдерского захвата также должна носить комплексный и динамический характер. В основе построения такой системы должны лежать представления о: мощности поля (среды) информационных угроз, номенклатуре информационных угроз, динамике изменения интенсивности угроз. Такое представление может быть получено путем построения модели динамической среды угроз информационной безопасности кредитно-финансового учреждения. Под динамической средой угроз информационной безопасности кредитно-финансового учреждения будем понимать составную часть внешней и внутренней среды функционирования кредитно-финансового учреждения, состоящую из разнородных информационных угроз, постоянно переходящих из потенциального состояния в реальное и обратно. Процесс преобразования потенциальных угроз в реальные, образующих в совокупности угрозу рейдерского захвата кредитно-финансового учреждения, будет определяться их жизненным циклом угрозы, схематично изображенным на рисунке (составлено авторами).

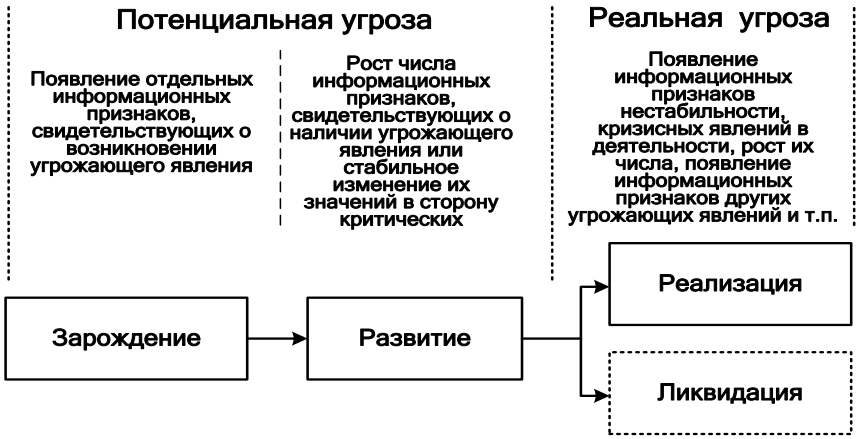

Рисунок. *Жизненный цикл угрозы*

Интенсивность преобразования потенциальных информационных угроз в реальные и их реализация будут зависеть от замысла и способа осуществления дестабилизирующих воздействий, которые могут описываться рядом параметров, образующих модель динамической среды угроз информационной безопасности кредитно-финансового учреждения.

Формализованное описание динамической среды угроз информационной безопасности кредитно-финансового учреждения (в канонической форме) представим в виде многомерного вектора $W_{<x>}$, включающего статические $W^{c}_{<x'>}$ и динамические $W^{\partial}_{<x''>}$ параметры: $W_{<x>} =< W^{(1)}_{<\ell_1>},...,W^{(x)}_{<\ell_x>},...,W^{(X)}_{<\ell_X>} >$, $W^{(x)}_{<\ell_x>}$ - 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 угроз, описываемых информационными признаками (информационно-признаковыми моделями), в совокупности образующих угрозу рейдерского захвата кредитно-финансового учреждения.

К основным статическим параметрам относятся:

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

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;
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 кредитно-финансового учреждения, так и вне него);
3. $W^{c(3)}_{<\ell_3>} = W^{c(3)}_{<7>} =< \omega^{c(3)}_1, \omega^{c(3)}_2,..., \omega^{c(3)}_7 >$ – характер объекта;
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;

5. $W^{c(5)}_{<\ell_5>} = W^{c(5)}_{<2>} =< \omega_1^{c(5)}, \omega_2^{c(5)} >$ – правовая база;
6. $W^{c(6)}_{<l_6>} = W^{c(6)}_{<3>} =< \omega_1^{c(6)}, \omega_2^{c(6)}, \omega_3^{c(6)} >$ – напряженность внутренней обстановки:
7. $W^{c(7)}_{<l_7>} = W^{c(7)}_{<3>} =< \omega_1^{c(7)}, \omega_2^{c(7)}, \omega_3^{c(7)} >$ – напряженность внешней обстановки:

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. $W^{\partial(1)}_{<h_1>} = W^{\partial(1)}_{<3>} =< \omega_1^{\partial(1)}, \omega_2^{\partial(1)}, \omega_3^{\partial(1)} >$ – темп развития внутренней угрозы;
2. $W^{\partial(2)}_{<h_2>} = W^{\partial(2)}_{<3>} =< \omega_1^{\partial(2)}, \omega_2^{\partial(2)}, \omega_3^{\partial(2)} >$ – темп развития внешней угрозы;
3. $W^{\partial(3)}_{<h_3>} = W^{\partial(3)}_{<3>} =< \omega_1^{\partial(3)}, \omega_2^{\partial(3)}, ..., \omega_7^{\partial(3)} >$ – этапы (фазы) развития угрозы рейдерского захвата;
4. $W^{\partial(4)}_{<h_4>} =< \omega_1^{\partial(4)}, \omega_2^{\partial(4)}, \omega_3^{\partial(4)} >$ – преследуемые цели;
5. $W^{\partial(5)}_{<h_5>} = W^{\partial(5)}_{<1>} =< \omega_1^{\partial(5)}, \omega_2^{\partial(5)}, \omega_3^{\partial(5)}, \omega_4^{\partial(5)} >$ – состав и возможности сил, формирующих угрозу;

Фрагмент перечня информационных аналогов угроз приведен в таблице (составлено авторами).

Таблица

Информационные аналоги параметров динамической среды угроз информационной безопасности (фрагмент)

Обозначение параметра	Информационный аналог (информационные признаки)
$\omega_1^{c(1)}$ – единичная угроза	сбой работы программного обеспечения компьютера (компьютер не выполняет команды, выполняет команды неправильно и т.п.); 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.
$\omega_2^{c(1)}$ – множественная угроза	сбой работы программного обеспечения нескольких компьютеров; выключение нескольких (или всех) компьютеров; поломка нескольких компьютеров; признаки несанкционированного доступа к информационным базам; постоянное появление посторонних лиц вблизи информационных хранилищ (узлов); непрофессиональные действия различных сотрудников и т.п.

$\omega_3^{c(1)}$ – концентрированное дестабилизирующее воздействие	совокупность информационных признаков единичных и множественных угроз на кратковременном интервале; наличие логической связи между информационными признаками множественных угроз; информационные признаки активных действий конкурирующих организаций и лиц и т.д.
……..	
$\omega_1^{\partial(1)}$ – высокий темп развития внутренней угрозы	частое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения.
$\omega_2^{\partial(1)}$ – средний темп развития внутренней угрозы	периодическое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения
$\omega_3^{\partial(1)}$ – низкий темп развития внутренней угрозы	редкое проявление информационных признаков внутренних целенаправленных единичной и множественной угрозы, дестабилизирующих воздействий и операций, основных причин их возникновения.

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

На основе предложенной модели динамической среды информационных угроз можно построить прогноз информационной обстановки кредитно-финансового учреждения. Качество данного прогноза зависит от своевременного определения состояния динамической среды угроз информационной безопасности кредитно-финансового учреждения. Для этого выделим N состояний динамической среды угроз информационной безопасности кредитно-финансового учреждения и обозначим их текущее состояние $A_i, i = \overline{1, N}.$.

Как уже упоминалось выше, каждое состояние динамической среды угроз информационной безопасности характеризуется своим набором информационных признаков. При этом в каждом состоянии динамической среды угроз информационной безопасности могут присутствовать информационные признаки m, характеризующие один из возможных несовместных вариантов (гипотез) реализации рейдерского захвата кредитно-финансового учреждения $S_j, \quad j = \overline{1, M}$: отсутствие мероприятий по рейдерскому захвату ($j = 1$); осуществление «белого» рейдерского захвата ($j = 2$); осуществление «серого» рейдерского захвата ($j = 3$); осуществление «черного» рейдерского захвата ($j = 4$). Многие события m могут появляться при любой из этих гипотез, поэтому вероятность события m вычисляется по формуле полной вероятности: $P(m) = \sum_{j=1}^{N} P(m/S_j)P(S_j)$, где: $P(S_j)$ – априорная вероятность того, что процесс рейдерского захвата кредитно-финансового учреждения находится в состоянии S_j (в качестве исходных данных может быть использовано значение $P(S_j) = 1/N$); $P(m/S_j)$ – условная вероятность проявления признака (проведения мероприятия) m при пребывании

процесса рейдерского захвата кредитно-финансового учреждения в состоянии S_j характеризующая силу соответствующей причинно-следственной связи.

При анализе поступающих данных большое значение имеет априорная информация о состоянии процесса. После получения новых сведений о проявившихся признаках (проведенных мероприятиях) апостериорное распределение вероятностей различных возможных состояний процесса рейдерского захвата кредитно-финансового учреждения может быть определено по формуле Байеса:

$$P(S_j/m) = \frac{p(S_j)\cdot P(m/S_j)}{\sum_{j=1}^{N} P(S_j)\cdot P(m/S_j)}$$

, где $P(S_j/m)$ – условная вероятность того, что процесс рейдерского захвата находится в S_j - м (из N возможных) состояний при проявлении признака (проведении мероприятия) m.

Таким образом, формула Байеса позволяет переоценить вероятности гипотез о состоянии процесса рейдерского захвата кредитно-финансового учреждения после того, как результаты наблюдения становятся известными.

Скорректированные вероятности самих гипотез $P(S_j/m)$ могут быть рассчитаны прямым образом (по формуле Байеса). При этом данная процедура является рекурсивной, т.е. если должно быть оценено более чем одно событие, то скорректированные вероятности гипотез при первой итерации становятся начальными вероятностями для очередной итерации.

Предложенная модель и методика ее реализации позволяют: по совокупности зафиксированных информационных признаков определить наличие и состояние угроз безопасности кредитно-финансового учреждения в целом, и информационных угроз, в частности; построить информационно-признаковые модели информационных угроз кредитно-финансового учреждения; определить интенсивность и динамику информационных угроз; сформировать исходные данные для построения эффективной и оптимальной системы защиты информации кредитно-финансового учреждения.

ЛИТЕРАТУРА

1. Вихорев С.В. Классификация угроз информационной безопасности. Cnews.ru годовой обзор «Сетевые атаки и системы информационной безопасности 2001» [Электронный ресурс] – URL: http://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf.
2. Галкова Е.А., Левкин И.М. Математическое описание динамической среды угроз информационной безопасности // Национальная безопасность и стратегическое планирование. – СПб: Информационный издательский учебно-научный центр «Стратегия будущего», 2014. - Вып. 5. - № 1. - С. 46-53.
3. Гацко М. О соотношении понятий «угроза» и «опасность». [Электронный ресурс] – Режим доступа: http://old.nasledie.ru/oboz/N07_97/7_06.HTM.
4. Ефимов А.Н. Информация: ценность, старение, рассеяние. – М.: Наука, 1983.
5. Жигулин Г.П. Теория и практика прогнозирования. – СПб: СПбНИУ ИТМО, 2011.
6. Конев И., Беляев А. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.: ил.
7. Левкин И.М. Теория и практика информационно-аналитической работы / И.М. Левкин. – Курск: НАУКОМ, 2011.
8. Левкин И.М., Сорокина Е.А. Рейдерский захват как особая форма информационно-экономической угрозы / И.М. Левкин, // 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.
9. Левкин И.М., Левкина С.В., Сорокина Е.А. Информационно-признаковое моделирование угроз национальной безопасности // Вестник Академии военных наук. Северо-Западное отделение, 2013.
10. Левкина С.В. Модели угроз экономической безопасности // XVI Всероссийская научно-практическая конференция «Актуальные проблемы защиты и безопасности» 3-6 апреля 2013. – СПб: РАРАН, 2013.
11. Ясенев В.Н. Информационная безопасность в экономических системах: Учебное пособие / В.Н. Ясенев. – Н. Новгород: Изд-во ННГУ, 2006.

Рецензент: Жигулин Георгий Петрович, доцент, к.т.н., декан факультета Институт комплексного военного образования ФГАОУ ВО Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, заведующий кафедрой Мониторинга и прогнозирования информационных угроз факультета Институт комплексного военного образования.

Galkova Elena Aleksandrovna
St. Petersburg national research university of information technologies, mechanics & optics
Russia, St. Petersburg
E-mail: sorokina_elena_@mail.ru

Levkin Igor Mikhaylovich
St. Petersburg national research university of information technologies, mechanics & optics
Russia, St. Petersburg
E-mail: lev.kin@yandex.ru

The model of the dynamic environment of information threats of financial institutions

Abstract. This article is described plural coordinated on goals, tasks, time and place of formation of threats of type the destabilizing concentrated effect. Example of such threats is the threat of raider seizure of financial institutions; this threat is accompanied by a breach information security. Also in the article are described peculiarities of formation of threats and building information security financial institutions, bearing a complex and dynamic in nature; is given the canonical description of the dynamic environment of information security threats of financial institutions; is presented a fragment of the description information of the characteristics of static and dynamic parameters of the developed model. Is concluded that the proposed model of the dynamic environment of information threats is distinguished a targeted search of additional (related) information attribute for more accurate identification of threats. The proposed model allows us: the first, to determine the presence and status of security threats financial institutions, including information threats; the second, to build information-indicative models of information threats financial institutions; the third, to determine the intensity and dynamics of information threats; the fourth, to form the source data for to build effective and optimal system of information security of financial institutions.

Keywords: information threat; security; financial institution; dynamic threat; dynamic environment; the intensity of threats; information attribute; static parameters threats; dynamic parameters threats; destabilizing concentrated effect.

REFERENCES

1. Vikhorev S.V. Klassifikatsiya ugroz informatsionnoy bezopasnosti. Cnews.ru godovoy obzor «Setevye ataki i sistemy informatsionnoy bezopasnosti 2001» [Elektronnyy resurs] – URL: http://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf.
2. Galkova E.A., Levkin I.M. Matematicheskoe opisanie dinamicheskoy sredy ugroz informatsionnoy bezopasnosti // Natsional'naya bezopasnost' i strategicheskoe planirovanie. – SPb: Informatsionnyy izdatel'skiy uchebno-nauchnyy tsentr «Strategiya budushchego», 2014. - Vyp. 5. - № 1. - S. 46-53.
3. Gatsko M. O sootnoshenii ponyatiy «ugroza» i «opasnost'». [Elektronnyy resurs] – Rezhim dostupa: http://old.nasledie.ru/oboz/N07_97/7_06.HTM.
4. Efimov A.N. Informatsiya: tsennost', starenie, rasseyanie. – M.: Nauka, 1983.
5. Zhigulin G.P. Teoriya i praktika prognozirovaniya. – SPb: SPbNIU ITMO, 2011.
6. Konev I., Belyaev A. Informatsionnaya bezopasnost' predpriyatiya. – SPb.: BKhV-Peterburg, 2003. – 752 s.: il.
7. Levkin I.M. Teoriya i praktika informatsionno-analiticheskoy raboty / I.M. Levkin. – Kursk: NAUKOM, 2011.
8. Levkin I.M., Sorokina E.A. Reyderskiy zakhvat kak osobaya forma informatsionno-ekonomicheskoy ugrozy / I.M. Levkin, // 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.
9. Levkin I.M., Levkina S.V., Sorokina E.A. Informatsionno-priznakovoe modelirovanie ugroz natsional'noy bezopasnosti // Vestnik Akademii voennykh nauk. Severo-Zapadnoe otdelenie, 2013.
10. Levkina S.V. Modeli ugroz ekonomicheskoy bezopasnosti // XVI Vserossiyskaya nauchno-prakticheskaya konferentsiya «Aktual'nye problemy zashchity i bezopasnosti» 3-6 aprelya 2013. – SPb: RARAN, 2013.
11. Yasenev V.N. Informatsionnaya bezopasnost' v ekonomicheskikh sistemakh: Uchebnoe posobie / V.N. Yasenev. – N. Novgorod: Izd-vo NNGU, 2006.