Николай С. Егошин, Антон А. Конев, Александр А. Шелупанов
Томский государственный университет систем управления и радиоэлектроники,
пр-т. Ленина, д. 40, г. Томск, 634050, Россия,
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701,
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956,
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ*

DOI: http://dx.doi.org/10.26583/bit.2017.4.02

Аннотация. Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности. Модель нарушителя является важной частью информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывает различные методы классификации нарушителей, меж тем многие специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы, так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. Несмотря на то, что многие модели имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось. В данной работе предпринимается попытка разработки своей собственной методики формирования модели нарушителя. Перед началом работы были сформированы следующие задачи научно-исследовательской работы: 1) изучить существующие методики построения модели нарушителя; 2) выявить недостатки существующих методик; 3) разработать модель нарушителя и методику составления перечня наиболее вероятных нарушителей, учитывающую выявленные недостатки. В ходе работы были проанализированы несколько существующих моделей нарушителя, в результате этого были выявлены их недостатки и определены сложности, на которые было обращено внимание при разработке собственной модели нарушителя. В разработанной модели были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий, описаны и ранжированы возможные виды предполагаемых нарушителей. Модель позволяет строить более полное описание нарушителя информационной безопасности.

Ключевые слова: модель нарушителя, модель угрозы, информационная безопасность, конфиденциальная информация.

Для цитирования. **ЕГОШИН, Николай С.; КОНЕВ, Антон А; ШЕЛУПАНОВ, Александр А.** ФОРМИРОВАНИЕ МОДЕЛИ НАРУШИТЕЛЯ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/273>. Дата доступа: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.02.

***Благодарности:** Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2017-2019 год (проект №2.8172.2017/8.9).

Nikolay S. Egoshin, Anton A. Konev, Alexander A. Shelupanov
Tomsk State University of Control Systems and Radioelectronics,
Lenin Av., 40 Tomsk, 634050, Russia
e-mail: ens@csp.tusur.ru, ORCID 0000-0003-4770-0701
e-mail: kaa@keva.tusur.ru, ORCID 0000-0002-3222-9956
e-mail: saa@keva.tusur.ru, ORCID 0000-0003-2393-6701

Building a model of infringer

DOI: http://dx.doi.org/10.26583/bit.2017.4.02

Abstract. By a model of infringer one means a set of assumptions about the specific (restricted) tools of the infringer, which the latter can use to conduct attacks. The infringer model is an important part of the organization's information security. One should realize that ignoring the model, or building it without due care, can seriously affect the security of confidential information and lead to its loss. The infringer model is informal, which implies the absence of strict and unambiguous methodology for developing such a model. There exist many academic and technical publications proposing various methods of classifying violators. Meanwhile, many information security practitioners are forced to create their own normative and methodological documents, because existing models do not necessarily capture all the aspects of the organization's work. Despite the fact that many models have a high level of correlation between classification characteristics, it has not been possible to work out a unified model so far. We attempt to develop our own methodology for building the infringer model. We have started this project by outlining the roadmap: (1) study the existing methods of constructing the infringer model; (2) identify shortcomings of existing methods; (3) develop a model of the infringer and a methodology for listing the most likely violators, with taking into account the identified shortcomings. In the process of implementation of the plan, we have analyzed several existing models of infringer and revealed their shortcomings and inherent difficulties. In the developed model, causal relationships between the elements of the model and the chains of the alleged consequences have been constructed, and possible types of alleged violators have been described and ranked. As a result, our model allows one to create a more deep description of the infringer.
Keywords: model of infringer, threat model, information security, confidential information

For citation. **EGOSHIN, Nikolay S; KONEV, Anton A; SHELUPANOV, Aleksander A.** Building a model of infringer. IT Security, [S.l.], v. 24, n. 4, p. 19-26, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/273>. Date accessed: 28 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.02.

***Acknowledgements:** The work was executed at financial support of the Ministry of education and science of the Russian Federation within the basic part of state task TUSUR in 2017-2019 year. (project No. 2.8172.2017/8.9).

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом автоматизированных систем (АС). С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений.

Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлении.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства [1].

Под моделью нарушителя понимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель нарушителя является важной частью в обеспечении информационной безопасности организации. Важно понимать, что игнорирование или недобросовестное построение модели «для галочки» может серьезно отразиться на сохранности конфиденциальной информации и привести к ее потере. Исходя из этого, решение

проблемных вопросов формирования модели нарушителя является одним из первоочередных и важных направлений обеспечения информационной безопасности.

Модель нарушителя носит неформальный характер, и, как следствие, не существует строго однозначной методики по составлению таковой. Множество авторов в научно-технической литературе описывает различные методы классификации нарушителей, несмотря на это, некоторые специалисты по информационной безопасности, работающие на предприятиях, вынуждены составлять свои нормативно-методические документы, так как существующие модели далеко не всегда удовлетворяют всем особенностям работы организации. И хотя большинство моделей и имеют высокий уровень корреляции между классификационными признаками, выработать единую модель до сих пор не удалось [2]. А между тем, существование единой универсальной модели имеет очевидное преимущество в виду того, что неполнота описания влечёт за собой необходимость доработки модели под нужды конкретной организации о чём было сказано ранее. Данное действие не всегда может быть корректно осуществлено по различным причинам (будь то недостаточный профессионализм сотрудника, либо банальная нехватка времени). Возможная избыточность модели не нанесёт вреда, в то время как пробелы в описании вероятных нарушителей могут оставить «дыры» в системе безопасности.

В данной работе осуществляется разработка своей собственной методики формирования модели нарушителя. Перед началом работы были сформированы следующие задачи научно-исследовательской работы:

1. изучить существующие методики построения модели нарушителя;
2. выявить недостатки существующих методик;
3. разработать модель нарушителя и методику составления перечня наиболее вероятных нарушителей, учитывающую выявленные недостатки.

В ходе работы были проанализированы несколько существующих моделей нарушителя, а именно: модель нарушителя по требованиям ФСТЭК России [3] и ФСБ России [4], модель нарушителя по требованиям руководящего документа Гостехкомиссии [5], модель угроз и нарушителя Минсвязи [6] и иные неформальные модели нарушителя [7, 8, 9, 10, 11, 12].

В результате анализа упомянутых моделей были выявлены их недостатки и определены сложности, на которые следует обратить внимание при разработке собственной модели нарушителя:

- некоторые модели рассматривают нарушителя исключительно как злоумышленника (например, [7]), мало упоминаний случайных ошибок, действий стихийного характера и природных явлений;
- модели представляют из себя описание примеров действий нарушителя, формулировки нередко многословны и сложны для восприятия;
- отсутствует универсальность разработанных моделей, например, модель [10] нельзя применить к системе, описываемой в работе [12] и наоборот;
- обширное использование лингвистических шкал оценок, что недопустимо для корректной оценки возможностей нарушителя.

Учитывая недостатки описанных ранее моделей можно составить перечень основных параметров нарушителя информационной безопасности, на основе которых будет строиться новая модель описания нарушителя:

Таблица 1 – Параметры нарушителя информационной безопасности

Параметр	Значение
M(otivation) – преднамеренность совершения нарушения	0-случайное, 1-преднамеренное
P(lace) – положение относительно организации, работающей с информацией	0-внешний, 1-внутренний
T(ype) – типнарушителя	4 типа на основе M и P (00, 01, 10, 11)
I(nformation) – знание рубежа защиты и уязвимости в нём	Отсутствие(0)/наличие (1)
E(xtra) – возможность использования несанкционированного средства обработки информации	Отсутствие(0)/наличие (1)
O(ff) – возможность отключения рубежа защиты	Отсутствие(0)/наличие (1)
D(isruption) – возможность нарушения работы рубежа защиты	Отсутствие(0)/наличие (1)
A(ttack) – возможность преодоления рубежа защиты	Отсутствие(0)/наличие (1)
Q(uality) – уровеньнарушителя	От 0 до 7 согласно схеме (рис.1)
Th(reat) – привязка к определенной угрозе	Отсутствие(0)/наличие (1)
N(umber) – количество рубежей защиты, которые осталось преодолеть	0-санкционированный пользователь, (число большее нуля) – несанкционированный

Условно параметры можно разделить на 2 части: а) параметры, описывающие тип (M, P и T) и качества нарушителя (I, E, O, D, A, Q); б) параметры, характеризующие систему защиты (Th и N).

Из схемы (рис. 1) видно, что в формируемой модели нарушителя произведено разделение:

- тип/качество нарушителя;
- поиск и использование уязвимости;
- произведено условное отделение санкционированных и несанкционированных действий и средств.

Для удобства пользователей данной модели нарушителя введена условная бальная система. По мере возрастания опасности от каждого нарушителя относительно каждого возможного действия поставлен определенный балл. Превосходство санкционированных средств над несанкционированными вызвано тем, что нарушитель, использующий санкционированные, то есть разрешенные самой системой, действия является гораздо более опасным, чем нарушитель, которому не хватает навыков и/или которому приходится использовать сторонние средства для достижения своей цели[13].

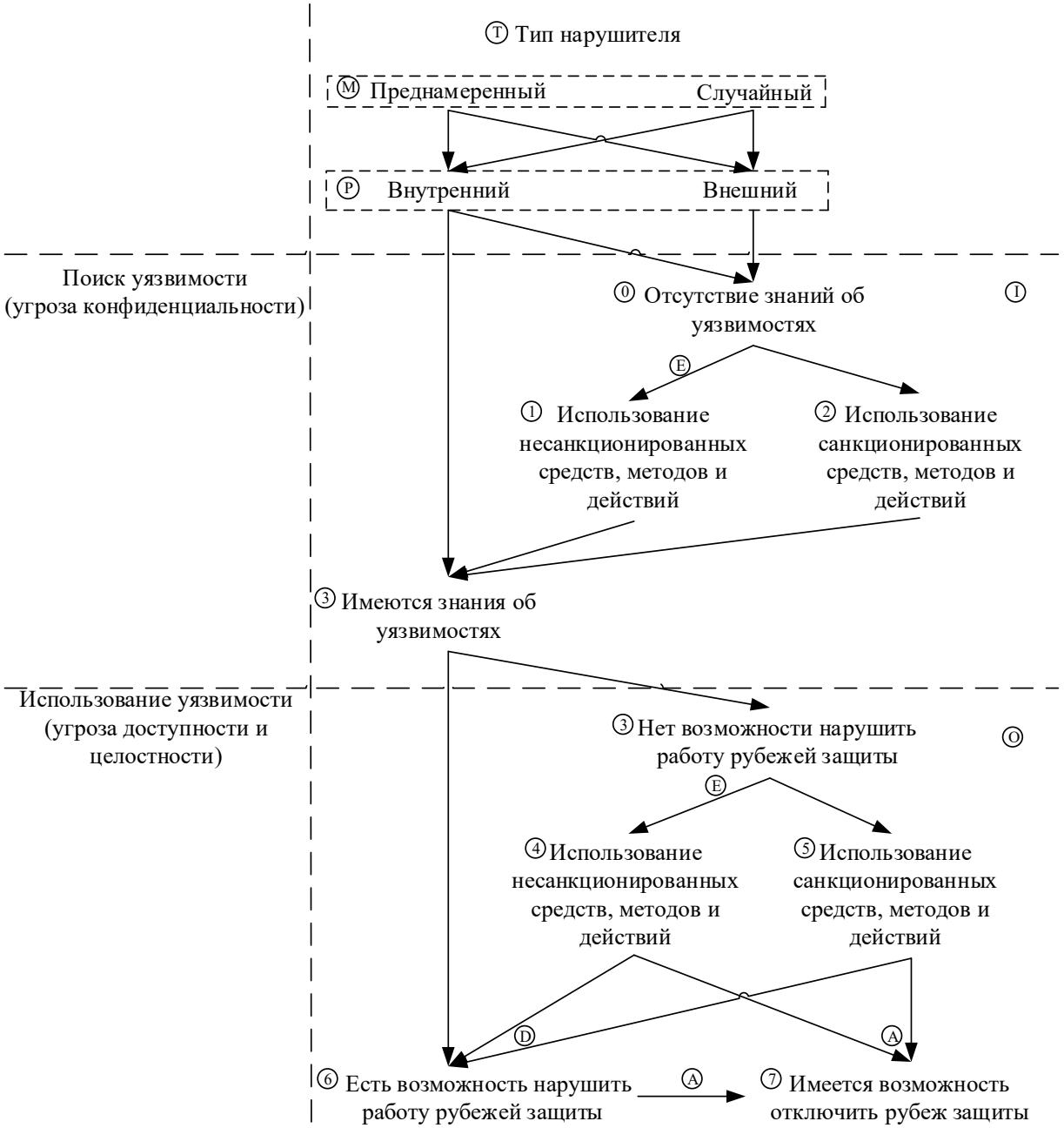

Рисунок 1 – Схема отображения параметров нарушителя
(Fig. 1 – Diagram display options of the offender)

Разделение же уровней нарушителя на поиск и использование уязвимостей вызвано тем, что действия нарушителя носят двойственный характер по отношению к информации о рубежах и к системе, в которой хранится конфиденциальная информация. Владея информацией об уязвимостях в рубежах, нарушитель может лишь рассказать эту информацию кому-либо, что само по себе представляет угрозу конфиденциальности. Имея же информацию об уязвимостях и в попытке ее использовать, нарушитель осуществляет угрозу доступности компонентов рубежа, целостности рубежа и всей системы в целом.

Разделение так же вызвано тем, что при каждом из этих действий нарушитель будет использовать разные средства: в первом случае нарушитель будет искать уязвимости, что больше носит пассивный характер, а во втором уже использовать, что носит уже гораздо более активный характер.

Исходя их этой схемы (рис. 1), можно сделать предположения о том, кем может являться нарушитель для каждого уровня, который на ней изображен:

0 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, (например, уборщица), у которых нет мотивации;

1 уровень – простой внешний либо внутренний нарушитель с очень ограниченным доступом, которые для выявления угроз используют несанкционированные средства для получения информации об уязвимостях в рубежах защиты. Например, следят за тем, что происходит в окнах здания из неконтролируемой территории;

2 уровень – нарушитель, который использует своё положение чтобы собирать информацию об уязвимостях в рубежах защиты, используя санкционированные методы. Например, ходить по зданию и высматривать положение камер наблюдения;

3 уровень – нарушитель, обладающий информацией об уязвимостях, может быть, как сотрудником, имеющим отношение к конструированию данного рубежа защиты, так и одним из нарушителей, ранее имевших 1 или 2 балла, при условии, что их действия не были замечены и пресечены сотрудниками охраны;

4 уровень – изначально внутренний нарушитель, имеющий достаточно информации про уязвимости в рубеже, но не имеющий возможности нарушить или преодолеть защиту рубежа, используя свой уровень допуска и использующий для этого несанкционированные средства. Примером может быть сотрудник, работающий на другом этаже здания с другим видом информации, но знающий общую схему здания, расположение и уязвимости в рубежах защиты. Этот сотрудник мог принести плоскогубцы и с их помощью вывести из строя камеры наблюдения. Перенося эту ситуацию в виртуальную среду можно сделать предположение, что потенциальным нарушителем может являться пользователь внутренней компьютерной сети здания, имеющий пароль для входа в операционную систему, но не имеющий доступа к определенной информации и использующий для этого программы-переборщики паролей;

5 уровень – изначально внутренний нарушитель, который для достижения своих целей использует санкционированные методы. Например, пользователь, имеющий пароль к необходимой информации может пересылать конфиденциальные данные другому санкционированному пользователю, работающему за территорией этого здания, например, в филиале, используя заведомо ненадежный канал передачи данных;

6 уровень – изначально внутренний нарушитель с высоким уровнем доступа, имеющий возможность нарушить работу рубежей защиты, пользуясь своим служебным положением. Таким сотрудником может быть администратор информационной безопасности;

7 уровень – изначально внутренний нарушитель с очень высоким уровнем доступа, имеющий возможность отключить рубеж защиты, используя своё служебное положение.

Таким сотрудником может являться администратор системы защиты либо работник охраны. Так же под это описание подходят форс-мажорные обстоятельства (например, природные катастрофы, так как природе перед стихийными бедствиями не нужно получать информацию о рубежах защиты и отключать их).

Следует также отметить, что привязка нарушителя осуществляется к угрозе, которая влияет непосредственно на информацию, остальные же пункты закреплены за охраняющими эту информацию рубежами защиты, так как при устранении всех рубежей информация автоматически становится доступной и тот, кто нарушил целостность рубежей получает ее в свое распоряжение[14].

Схематически работу предлагаемой методики формирования модели нарушителя с использованием известной из системного анализа модели черного ящика можно представить следующим образом (рис. 2).

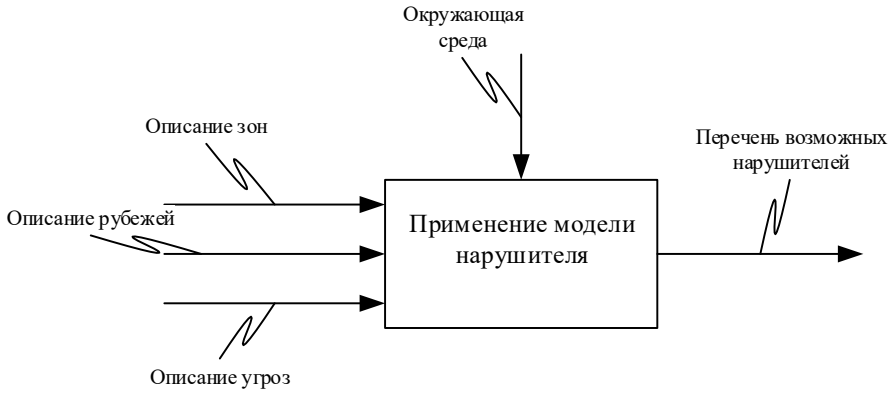

Рисунок 2– Схематическое описание работы модели нарушителя безопасности с использованием черного ящика
(Fig. 2– Schematic description of the operation of the intruder model security using the black box)

В итоге, методика формирования модели нарушителя действует следующим образом:

1. описываются все зоны, окружающие конфиденциальную информацию[15];
2. описываются все рубежи защиты между зонами и внутри них[15];
3. описываются возможные угрозы;
4. описывается состояние окружающей среды;
5. приведенные описания применяется к схеме (рис. 1)в результате чего формируется и получается описание вероятных нарушителей информационной безопасности.

Таким образом, в разработанной модели были построены причинно-следственные связи между элементами модели и цепочками предполагаемых последствий. Основываясь на этом, а также на описании состояния окружающей среды, рубежей защиты и всех зон, окружающих конфиденциальную информацию, были описаны и ранжированы возможные виды предполагаемых нарушителей. Как следствие, модель позволяет построить полное и универсальное по отношению к различным системам описание вероятного нарушителя информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1 Герасименко В. А. Основы защиты информации в автоматизированных системах: В 2 кн. – Кн. 2. – М.: Энергоатомиздат, 1994. – 176 с.

2 Стефаров А. П., Жукова М. Н. О сравнении моделей нарушителя правил разграничения доступа в автоматизированных системах. Информационное противодействие угрозам терроризма. 2013. № 20. С. 147-151.

3 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка): методика, утв. ФСТЭК России 15.02.2008. Собрание законодательства. 2008. 156 с.

4 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [Текст] : утв. Руководством 8 Центра ФСБ России 21 февр. 2008 года № 149/54-144. – М., 2008. – 20 с.

5 Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: руководящий документ, утв. РД Гостехкомиссии 30.03.1992.

6 Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли: методика, одобрено секцией №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21.04.2010.

7 Белоножкин В. И. Модель нарушителя безопасности региональной антитеррористической ИАС. Информация и безопасность. 2006. № 2. С. 155-157.

8 Федюнина А. П., Коломина И. В. Неформальная модель нарушителя в информационной сфере. Вестник Астраханского государственного технического университета. 2007. № 3. С. 166-168.
9 Гришина Н. В. Модель потенциального нарушителя объекта информатизации. Известия ЮФУ. Технические науки. 2003. С. 356-358
10 Аютова И. В. Модель нарушителя безопасности ВУЗа. Сборники конференций НИЦ Социосфера. № 8. 2012. С. 372-388.
11 Чебанов А.С., Жук Р.В., Власенко А.В., Сазонов С.Ю. Модель нарушителя комплексной системы обеспечения информационной безопасности объектов защиты. Известия Юго-Западного государственного университета. Серия: управление, вычислительная техника, информатика, медицинское приборостроение. 2013. № 1. С. 171-173.
12 Десницкий В.А., Чеулин А.А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами. Технические науки – от теории к практике. 2014. № 39. С. 7-21.
13 Novokhrestov A., Konev A. Mathematical model of threats to information systems. AIP conference proceedings. 2016. vol. 1772. pp. 060015.
14 Скрыль С. В., Исаев О. В. Имитационное моделирование процесса преодоления «моделью» нарушителя комплексов средств охраны. Вестник Воронежского института ФСИН России. 2013. № 1. С. 65-67.
15 Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации. Доклады ТУСУР. 2013. №2(28). С. 107–111.

REFERENCES:

[1] Gerasimenko V. A. Basics of information protection in automated systems: In 2 books – Book 2. – M.: Jenergoatomizdat, 1994. – 176 p. (in Russian).
[2] Stefarov A. P., Zhukova M. N. On comparing models of rule-breaker access security in automated systems. Informacionnoe protivodejstvie ugrozam terrorizma. 2013. № 20. P. 147-151. (in Russian).
[3] Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh (vypiska): metodika, utv. FSTJeK Russia. 15.02.2008 // Sobranie zakonodatel'stva. 2008. 156 p. (in Russian).
[4] Metodicheskie rekomendacii po obespecheniju s pomoshh'ju kriptosredstv bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh s ispol'zovaniem sredstv avtomatizacii [Tekst] : utv. Rukovodstvom 8 Centra FSB Rossii 21 fevr. 2008 goda № 149/54-144. – M., 2008. – 20 p. (in Russian).
[5] Koncepcija zashhity sredstv vychislitel'noj tehniki i avtomatizirovannyh sistem ot nesankcionirovannogo dostupa k informacii: rukovodjashhij dokument, utv. RD Gostehkomissii 30.03.1992. (in Russian).
[6] Model' ugroz i narushitelja bezopasnosti personal'nyh dannyh, obrabatyvaemyh v tipovyh informacionnyh sistemah personal'nyh dannyh otrasli: metodika, odobreno sekciej №1 Nauchno-tehnicheskogo soveta Minkomsvjazi Rossii «Nauchno-tehnicheskoe i strategicheskoe razvitie otrasli» ot 21.04.2010. (in Russian).
[7] Belonozhkin V. I. Model intruder security regional counter-terrorism IAS. Informacija i bezopasnost'. 2006. № 2. P. 155-157. (in Russian).
[8] Fedjunina A. P., Kolomina I. V. An informal model of the intruder in the field of information. Vestnik Astrahanskogo gosudarstvennogo tehnicheskogo universiteta. 2007. № 3. P. 166-168. (in Russian).
[9] Grishina N. V. Model potential intruder object of Informatization. Izvestija JuFU. Tehnicheskie nauki. 2003. P. 356-358. (in Russian).
[10] Ajutova I. V. Model of the offender security of the University. Sborniki konferencij NIC Sociosfera. № 8. 2012. P. 372-388. (in Russian).
[11] Chebanov A.S., Zhuk R.V., Vlasenko A.V., Sazonov S.Ju. The intruder model complex systems of information security protection. Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta. Serija: upravlenie, vychislitel'naja tehnika, informatika, medicinskoe priborostroenie. 2013. № 1. P. 171-173. (in Russian).
[12] Desnickij V.A., Cheulin A.A. A generalized model of the offender and verification of information and telecommunication systems with embedded devices. Tehnicheskie nauki – ot teorii k praktike. 2014. № 39. P. 7-21. (in Russian).
[13] Novokhrestov A., Konev A. Mathematical model of threats to information systems // AIP conference proceedings. 2016. vol. 1772. pp. 060015.
[14] Skryl' S. V., Isaev O. V. Simulation of the process of overcoming a "model" offender of complexes of means of protection. Vestnik Voronezhskogo instituta FSIN Rossii. 2013. № 1. P. 65-67. (in Russian).
[15] Konev A.A., Davydova E.M. Approach to the description of the structure of information security system. Doklady TUSUR. 2013. №2(28). P. 107–111. (in Russian).

Поступила в редакцию – 03 августа 2017 г. Окончательный вариант – 09 ноября 2017 г.
Received – August 03, 2017. The final version – November 09, 2017.