АЛГОРИТМ РАСЧЁТА ИНТЕГРИРОВАННОГО ПОКАЗАТЕЛЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Исаев А.Б.[1], Алнадфа А.[2], Исаев И.А.[3]

В работе рассматривается проблема незаконного проникновения в некоторую информационную систему и, кроме этого, проблема незаконного проникновения в кабинет руководителя предприятия. В первом случае рассмотрена распределенная информационно–управляющая система (ИУС), приведена её структурная схема, приведены каналы утечки, получены численные оценки для вероятностей несанкционированного доступа по этим каналам в ИУС, рассчитана привлечением логической функции движения информации по этой системе – усредненная вероятность «взлома» данной ИУС. Кроме того, изучен процесс проникновения злоумышленника с неохраняемой территории внутрь помещения, где находится кабинет руководителя, содержащий информацию, интересующую злоумышленника. Разработана графическая модель проникновения злоумышленника в данный кабинет, по которой рассчитана оценка для вероятности проникновения в этот кабинет, косвенно характеризующая ущерб от проникновения. По предложенным алгоритмам могут быть рассчитаны вероятности взлома (ущерба) от различных сценариев, реализуемых злоумышленником. Поэтому основной целью результатов исследования, представленного в данной работе, является изложение оригинального алгоритма, в общем случае позволяющего рассчитать определенным образом усреднённый показатель, равный вероятности взлома всей системы в целом, включая «взлом» каждого её блока или трактов передачи информации с помощью конструирования логической функции, соответствующей каждой индивидуальной процедуре незаконного проникновения в любую информационную систему. Если интересует взлом какого–либо тракта движения информации (с определенным образом соединенными элементами), то вероятности этой угрозы будет соответствовать, естественно, другая логическая функция и результат её использования предоставит исследователю так же «усреднённый» (интегральный) по всему выбранному «пути» перемещения злоумышленника показатель. Хочется отметить оригинальность и некоторую самобытность полученных результатов, к сожалению, не встретившихся авторам в современной специальной литературе.

***Ключевые слова**: информационно–управляющая система, логическая функция, структурная схема, каналы утечки, вероятность взлома, движение информации, злоумышленник.*

DOI:10.21681/2311-3456-2016-5-15-20

Введение

В виду всё возрастающего объема внедряемых в наше общество новых информационных технологий, в условиях массового использования персональных компьютеров, наличия технического оборудования от разных производителей, постоянный рост объема и сложности программного обеспечения, рост степени распределённости систем и прочее - вот далеко не полный перечень факторов, провоцирующих вероятность незаконного проникновения в любой объект или систему, в том числе в систему информационной безопасности объекта.

Рассматриваемая в статье проблема и связанные с ней практические задачи целиком находятся в классе задач по моделированию угроз воздействия на все возможные источники информации: моделирование способов проникновения к местам скопления информации (например, кабинет кого-либо из руководителей предприятия, генерального директора крупного производственного объединения); моделирование оптических каналов утечки (окна, двери, закладное устройство) - этот перечень может быть существенно увеличен [1-8].

Заметим, что традиционно считается, что большинство задач инженерно-технической защиты являются слабо формализуемыми задачами, когда формальное получение оптимального решения крайне затруднительно в виду наличие большого числа факторов самой различной природы, в очень малой степени поддающихся точному учету и корректному описанию из-за малого объема необходимой информация об этих факторах.

1 Исаев Андрей Борисович, кандидат технических наук, доцент, Финансовый университет при правительстве РФ, Москва, a.borisovich2010@yandex.ru

2 Алнадфа Антуан, РУДН, Москва, antwan.tiger@gmail.com

3 Исаев Иван Андреевич, РУДН, Москва

Однако, в данной работе эта трудность преодолеваются, если рассматривать оценку вероятности взлома информационной системы в рамках нетрадиционного системного подхода, который может быть реализован в виде некоторой структурные схемы, где в роли блоков выступают отдельные каналы незаконного проникновения в систему.

Модельное описание

Сама задача интегрального оценивания «взлома» всей системы (всех её блоков, элементов) решается оригинальным способом составления логической функции, описывающей процедуру незаконного проникновения в систему (в каждый её элемент, в тракты передачи информации). Далее составленная функция должна приводиться к ее «минимальной форме» и заменяться на «арифметическую» логическую функцию. При этом каждому блоку (элементу) логической функции «взлома» системы должна быть приписана некоторая его индивидуальная вероятность несанкционированного проникновения через данный блок (Рівзл, і – номер блока).

Далее необходимо следовать строго по пунктам алгоритма авторов.

Сформулировать словесно условия несанкционированного проникновения в информационную систему «взламывания» всех элементов (блоков) и связанных с ними трактов движения информации по системе от первого («входного») блока до последнего «выходного» блока.

На основе словесной формулировки или ее соответствующей структурной схемы необходимо составить и записать логическую функцию Fпвзл как «высказывание» относительно процедуры «взламывания» всех элементов системы и её трактов передачи информации, соединяющих эти блоки (если в этом есть необходимость).

Используя набор известных логических постулатов (см. [9, с.132]), привести полученную логическую функцию к её «минимальной» «бесповоротной» форме.

Перейти от данной функции к «арифметической» логической функции, содержащей численные оценки вероятности «взлома» всех элементов системы.

Выполнив все необходимые арифметические действия, получить некий «усредненный» определенным образом «интегральный показатель», численно равный вероятности «взлома» всех блоков (элементов) исследуемой системы.

В работе этот показатель будет получен для некоторой распределенной информационной управляющей системы (ИУС), а также для взятого из [10, с.656] примера моделирования «угроз» в кабинете руководителя будет получена оценка вероятности незаконного проникновения в кабинет руководителя предприятия с целью хищения в служебной информации.

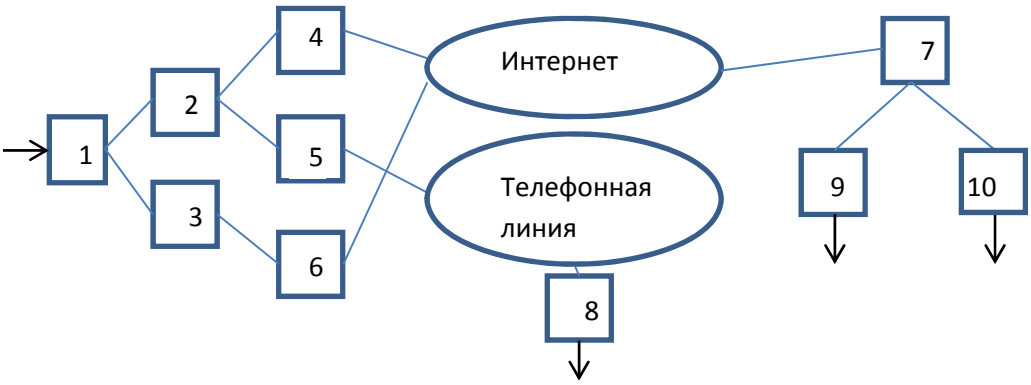
Очевидно, что вводимый таким образом показатель (обозначим его L) носит интегральный характер и находится целиком в рамках интегрального подхода к проблеме защиты информации, в рамках концепции интегральной безопасности. Известно, что интегральная безопасность характеризует такое физическое состояние функционирующего объекта, циркулирующей в нем информации и человеческого фактура, при котором они надежно защищены от всех возможных видов угроз несанкционированного доступа, под НСД к ресурсам компьютерной системы понимаются действия по использованию, изменению и уничтожению используемых данных указанной системы, производимые субъектом, не имеющим права на такие действия [11, с.21], [13, с. 256] в процессе решения поставленных задач.

Интегральная безопасность, в пределе, должна аккумулировать в себе как все необходимые для решения данной задачи на объекте виды безопасности (охранная, пожарная, электрическая, экологическая, информационная и т.д.), так и перечень большинства каналов утечки рассматриваемого объекта (акустического, электрического, электромагнитного и т.д.) для их блокировки.

В настоящее время считается общепризнанным фактом, что, оставаясь в рамках концепции интегральной защиты, интегральной безопасности объекта, эффективность создаваемой системы информационной безопасности этого объекта может быть существенно повышена.

Вводимый интегральный показатель L находится полностью в рамках системного подхода к рассматриваемой в статье задаче оценивания вероятности взлома системы защиты информации, поскольку этот показатель рассчитывается на основе наиболее универсальной модели объектно-структурной схемы системы информационной безопасности.

В рассматриваемой нами задаче - моделировании процессов взлома системы информационной безопасности - в качестве элементов такой системы естественно рассматривать возможные каналы утечки информации, представляемые в виде блоков структурной схемы, соединенных последовательно, параллельно, треугольником, звездой и другими стандартными способами.



В случае отсутствие необходимой структурной схемы, процедура моделирования начинается с выделения некоторого конечного числа каналов утечки, например: электрического, акустического, электромагнитного, кабельной сети и двух компьютеров (с их материнскими платами). Можно предложить следующую формулировку процедуры несанкционированного проникновения в систему информационной безопасности.

Рассмотрим распределенную ИУС, состоящую из центра управления 1, сервера обработки почты 2, связи через телефонную линию интернет, удаленного сервера 7,8, рабочие станции конечных пользователей 9, 10, шлюз 4, вспомогательный шлюз 5, Intranet сервер 3, File server 6.

Из литературных данных [9, 10] нами были взяты следующие каналы утечки для блоков (1-10) и оценки для соответствующих вероятностей несанкционированного доступа в систему посредством этих каналов.

Блок 1 - электрический канал утечки P≅0.1

Блоки 2,6,7,8 - использование вирусных программ для несанкционированного доступа в систему P≅0.08

Блок 3 - электромагнитный канал утечки P≅0.18

Блоки 4,5 - электрический канал утечки P≅0.15

Блок 9,10 - использование вирусных программ для несанкционированного доступа в систему P≅0.3

Телефонная линия - акустический канал утечки P≅0.45

Интернет линия - электромагнитный канал утечки P≅0.35

Для получения интегральной экспертной оценки несанкционированного доступа в систему составляем логическую функцию движения информации в рассматриваемой системе:

L∑=P(l)*P(2)*P(4)*P(int)*P(7)*P(9) ∪ P(l)*P(2)* *P(4)*P(int)*P(7)*P(10) ∪ P(l)*P(2)*P(5)*P(tel)*P(8) ∪ ∪ P(l)*P(3)*P(6)*P(int)*P(7)*P(9) ∪ P(1)*P(3)*P(6)*P(int)*P(7)*P(10)

L∑=P(l)*P(2)*P(4)*P(int)*P(7)*(P(9) ∪P(10)) ∪ P(l)* *P(2)*P(5)*P(tel)*P(8) ∪ P(l)*P(3)*P(6)*P(int)*P(7)*(P(9) ∪P(10))

Для упрощения вида выражения примем:

A1= P(l)*P(2)*P(4)*P(int)*P(7)

A2= P(l)*P(2)*P(5)*P(tel)*P(8)

A3= P(l)*P(3)*P(6)*P(int)*P(7)

Переходя к арифметической логической функции:

La = A1*(P(9) ∪P(10)) + A2+ A3*(P(9) ∪P(10)) - A1* *A2*(P(9) ∪P(10)) - A2* A3*(P(9) ∪P(10)) - A1* A3*(P(9) ∪P(10))2 + A1* A2*A3*(P(9) ∪P(10))2

Таким образом:

A1= 0,1*0,08*0,15*0,35*0,08=0,0000336

A2= 0,1*0,08*0,15*0,45*0,08=0,0000432

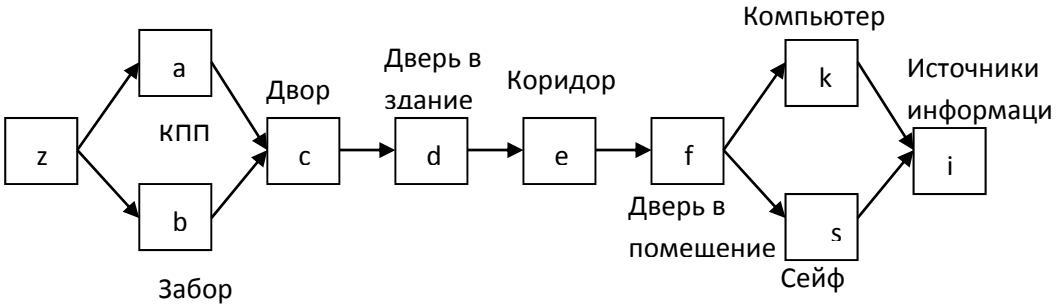
A3= 0,1*0,18*0,08*0,35*0,08=0,0004032

La = 0,0000336*(0,3+0,3-0,09)+ 0,0000432+ +0,0000432*(0,3+0,3-0,09)- -0,0000336*0,0000432*(0,3+0,3- -0,09)- 0,0000432*0,0004032*(0,3+0,3- 0,09)- 0,0000336*0,0004032*(0,3+0,3- 0,09)2+0,0000336*0,0000432*0,0004032* (0,3+0,3-0,09)2≅0,000266.

В принципе, не следует переоценивать малую величину вероятности «взлома» всей системы целиком, со всеми элементами, ибо метод расчета учитывает всё количество вариантов несанкционированного доступа в данную систему, и в логической функции в явном виде присутствуют вероятности «взлома» каждого из элементов информационной системы.

Рассчитанный показатель, характеризующий надежность системы от «взлома», должен учитываться при аттестации любой информационной системы.

Рассмотрим другой практический пример, связанный с моделированием угроз для информации, сосредоточенной на носителях в кабинете руководителя [10, с.768].



При моделировании подобного рода угроз необходимо прогнозировать маршрут движения злоумышленника, от злоумышленников исходят угрозы безопасности, которые могут быть связаны, как с особенностями функционирования компьютерных сетей (логическими и физическими), так с ошибками в реализации тех или иных функций по работе с информацией [12, с.250], находящегося вне территории организации, к источникам информации в кабинете руководителя.

Графическая модель проникновения злоумышленника в несколько упрощенном виде взято из [10, с.564].

Z – злоумышленник;

Pz-a – злоумышленник примет решение о «проходе» через КПП;

Pz-b – злоумышленник примет решение о проникновении через забор;

Pa – вероятность незаконного проникновения через КПП;

Pb – вероятность проникновения через забор;

Pc – вероятность проникновения через двор;

Pd – вероятность проникновения через дверь в здание;

Pe – вероятность проникновения через коридор;

Pf – вероятность проникновения через дверь в помещение, где находится кабинет руководителя;

Pk – вероятность взлома компьютера руководителя;

Ps – вероятность взлома сейфа руководителя;

Pi – вероятность хищения прочих источников информации;

Примем следующие оценки вероятностей на основании рекомендаций из [10]:

Pz-a≅0,1; Pz-b≅0,9; Pa≅1*10-3; Pb≅1*10-2; Pc≅0,5; Pd≅0,4; Pe≅0,3; Pf≅1*10-4; Pk≅0,1; Ps≅1*10-5; Pi≅0,5;

Lвзл=Pz-a*Pa*Pc*Pd*Pe*Pf*(Pk*Ps)*Pi ∪ Pz-b*Pa**Pc*Pd*Pe*Pf*Pk*Ps*Pi;

Обозначим:

A=Pa*Pc*Pd*Pe*Pf*Pk*Ps*Pi;

Тогда:

La=Pz-a*A ∪ Pz-b* A ⇒ A(Pz-a ∪ Pz-b);

Переходя к арифметической логической функции:

La=A(Pz-a+Pz-b- Pz-a*Pz-b);

A = 10-3 * 0,5 * 0,4 * 0,3* 10-4* 0,1* 10-5* 0,5= 10--3* 5* 10-1* 4* 10-1*3* 10-1*10-4*10-1*10-5*5* 10--1=300*10-4*10-6*10-7=3*102*10-17=3*10-15;

La=3*10-15*(0,1+0,9-0,09)= 3*10-15*0,91=2,73**10-15 – это оценка вероятности проникновения в кабинет, и косвенная оценка «ущерба» от этого факта.

В принципе, можно моделировать различные сценарии проникновения злоумышленника, например, проникновение в кабинет руководителя во внерабочее время или в ночное время, задаваясь другими числовыми параметрами. Можно вводить еще другие варианты сценария – например, с закладным устройством или окном в кабинете руководителя и т.д.

Корректность результата зависит от используемых численных значений вероятностей всех учтенных событий.

Заключение

В заключение заметим, что вопрос о полной группе «событий» решается очевидно: в последнем случае событие: вероятность проникновения в кабинет руководителя - $P_{взл}$=2,73*10-15, а ему противоположное событие это $\bar{P}_{взл}$=1-2,73*10-15 – т.е. «надежность» системы, и оба события составляют полную группу событий последний задачи.

Интересно опробовать данную методику в ситуации, близкой к инженерной, на примере анализа работы стандартной мостовой схемы, чаще других встречающейся в задачах теории надежности и кибернетике.

Если рассматриваемая кибернетическая система удовлетворительно аппроксимируется схемой моста, то возьмем за основу расчетов следующую структуру (мост)

Где, a,b,c,d,e – необходимые элементы моста.

Вероятность его работоспособного состояния, или надежность, дается следующей логической функцией

L∑ = (a*d) V (a*c*e) V (b*e) V (b*c*d) => c*{(a*d) V (a*e) V (b*e) V (b*d) } V not c*{ a*d V b*e } => c*{(d V e)*a V b* (d V e) } V not c*{ a*d V b*e } => c*{ (a V b) (d V e) } V not c*{d*a V b*e}.

Переходя к арифметической функции и взяв

Pa = Pb = …. = Pe = 0,99 получим

Fa = c*{(a + b - a*b) * (d + e - d*e)} + (1-c)*{(a*d + +b*c – a*d*b*c)} = 0,9998.

Для получения интегральной экспертной оценки несанкционированного доступа, подставим в выражение для арифметической логической функции Fa численное значение вероятности несанкционированного доступа, например, равное 0,01 повсюду (случайный приблизительный выбор) и выполним расчеты, попрежнему, со схемой моста.

Fa = Рвзл =0,01 [(0,02 - 0,0001)2] + 0,99(1, 10-4+ +1, 10-4 - 1, 10-8) = 0,01* 0,01992 + 0,99 * (2, 10-4 – -1, 10-8) = 0,01 * 0,0004 + 0,99 . 0,0002 = 0,000004 + +0,000198 = 0,000202.

Таким образом, усреднённая согласно логической функции и называемая нами интегральной экспертной оценкой равна 2,02*10-4 .

Отметим, что приводимые литературные ссылки содержат совершенно оригинальный информационный материал, нигде более не публиковавшийся, а приведенная графическая модель, соответствующая проникновению злоумышленника в кабинет руководителя, взята в немного упрощенном виде из [10, с.564].

Выводы

Получена распределенная информационно-управляющая система (ИУС), приведена её структурная схема, приведены каналы утечки, получены численные оценки для вероятностей несанкционированного доступа по этим каналам в ИУС.

Рассчитана усредненная вероятность «взлома» данной ИУС.

Изучен процесс проникновения злоумышленника с неохраняемой территории внутрь помещения, где находится кабинет руководителя, содержащий информацию, интересующую злоумышленника. Разработана графическая модель проникновения злоумышленника в данный кабинет, по которой рассчитана оценка для вероятности проникновения в этот кабинет.

***Рецензент**: Фильченков Михаил Леонидович, доктор физико-математических наук, профессор РУДН, fmichael@mail.ru*

Литература

1. Белокуров С.В., Зыбин Д.Г., Кондратов О.А., Змеев А.А. Математическое моделирование показателей защищенности информационных процессов в инфокоммуникационных системах // Вестник Воронежского института ФСИН России. 2014. № 2. С. 19-23.
2. Глыбовский П.А., Глухов А.П., Пономарев Ю.А., Шиленков М.В. Подход к оцениванию и прогнозированию уровня защищенности информационных и телекоммуникационных систем // Труды СПИИРАН. 2015. № 5 (42). С. 180-195.
3. Казарин О.В., Кондаков С.Е., Троицкий И.И. Подходы к количественной оценке защищенности ресурсов автоматизированных систем // Вопросы кибербезопасности. 2015. № 2 (10). С. 31-35.
4. Коломиец В.В. Метод получения вербальных показателей защищенности системы // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2014. Т. 12. № 2. С. 42-47.
5. Курочкин С.И., Заводцев И.В. Методы оценки уровня защищенности информационных систем // Перспективы развития информационных технологий. 2016. № 29. С. 197-204.
6. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. № 1 (14). С. 17-23.
7. Чобанян В.А., Шахалов И.Ю., Райков О.В. Некоторые аспекты расчета эффективности средств защиты информации перспективных автоматизированных систем военного назначения // Известия Российской академии ракетных и артиллерийских наук. 2014. № 3. С. 35-38.
8. Язов Ю.К., Машин О.А., Платонов Б.Ф. К вопросу об оценке эффективности выборочного контроля защищенности информации в информационных системах от несанкционированного доступа // Вопросы кибербезопасности. 2015. № 3 (11). С. 15-22.
9. Исаев А.Б. Современные технические методы и средства защиты информации. М.: РУДН, 2008. 253 с.
10. Торокин А.А. Инженерно-техническая защита информации М.: Гелиос АРВ, 2005. 960 с.
11. Барсуков В.С. Безопасность: технологии, средства, услуги. М.: Кудиц-Образ, 2011. 500 с.
12. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. СПБ.: НИУ ИТМО, 2012. – 418 с.
13. Атагимова Э.И., Макаренко Г.И., Федичев А.В. Информационная безопасность. Терминологический словарь в определениях действующего законодательства. М: ФБУ НЦПИ при Минюсте России, 2015. 448 с.

THE ALGORITHM FOR CALCULATING THE INTEGRATED INDICATOR OF SECURITY OF INFORMATION SYSTEMS AGAINST UNAUTHORIZED ACCESS

Isaev A.B.[4] , Alnadfa A.[5] , Isaev I.A.[6]

Our work deals with the problem of illegal entry into some information system and, in addition, the problem of illegal penetration into the office of the director. In the first case, the distribution management information system (MIS), shows its block diagram shows the leakage channels, obtained numerical estimates for the probability of unauthorized access to these channels in the ISC, designed involving logic function of motion information on this system – the average probability of «hacking» this MIS. In addition, we studied the intruder penetration process with an unguarded area inside the room, where the head office, containing information of interest to the attacker. A graphic model of the attacker's penetration in this study, which is designed for the evaluation of the probability of penetration in the office, indirectly characterizing the damage caused by penetration. According to the proposed algorithm can be calculated probability of breaking (damage) of the various scenarios to be implemented by the attacker. Therefore, the main purpose of the research results presented in this paper is to describe the original algorithm, in general, allows you to calculate a certain way averaged score of probability of breaking the system as a whole, including «hacking» of each of its block or data transmission paths using the design logic function corresponding to each individual procedure unlawful entry into any information system. If you are interested in breaking any path of motion information (with a certain way of combining the elements), the probability of this threat will meet, naturally, the other logical function and the result of its use will provide the researcher as «averaged» (integrated) over the selected «path» movement attacker indicator. It should be noted the originality and identity of some of the results, unfortunately, are not encountered authors in modern literature.

***Keywords**: information management system, a logical function, block diagram of the channels of leakage, the probability of hacking the movement of information, threat modeling effects, graphic model, an attacker.*

References

1. Belokurov S.V., Zybin D.G., Kondratov O.A., Zmeev A.A. Matematicheskoe modelirovanie pokazateley zashchishchennosti informatsionnykh protsessov v infokommunikatsionnykh sistemakh, Vestnik Voronezhskogo instituta FSIN Rossii. 2014, No 2. S. 19-23.
2. Glybovskiy P.A., Glukhov A.P., Ponomarev Yu.A., Shilenkov M.V. Podkhod k otsenivaniyu i prognozirovaniyu urovnya zashchishchennosti informatsionnykh i telekommunikatsionnykh sistem, Trudy SPIIRAN. 2015, No 5 (42). S. 180-195.
3. Kazarin O.V., Kondakov S.E., Troitskiy I.I. Podkhody k kolichestvennoy otsenke zashchishchennosti resursov avtomatizirovannykh sistem, Voprosy kiberbezopasnosti. 2015, No 2 (10). S. 31-35.
4. Kolomiets V.V. Metod polucheniya verbal'nykh pokazateley zashchishchennosti sistemy, Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii. 2014. T. 12, No 2. S. 42-47.
5. Kurochkin S.I., Zavodtsev I.V. Metody otsenki urovnya zashchishchennosti informatsionnykh sistem, Perspektivy razvitiya informatsionnykh tekhnologiy. 2016, No 29. S. 197-204.
6. Olad'ko V.S. Model' vybora ratsional'nogo sostava sredstv zashchity v sisteme elektronnoy kommertsii, Voprosy kiberbezopasnosti. 2016, No 1 (14). S. 17-23.
7. Chobanyan V.A., Shakhalov I.Yu., Raykov O.V. Nekotorye aspekty rascheta effektivnosti sredstv zashchity informatsii perspektivnykh avtomatizirovannykh sistem voennogo naznacheniya, Izvestiya Rossiyskoy akademii raketnykh i artilleriyskikh nauk. 2014, No 3. S. 35-38.
8. Yazov Yu.K., Mashin O.A., Platonov B.F. K voprosu ob otsenke effektivnosti vyborochnogo kontrolya zashchishchennosti informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa, Voprosy kiberbezopasnosti. 2015, No 3 (11). S. 15-22.
9. Isaev A.B. Sovremennye tekhnicheskie metody i sredstva zashchity informatsii. M.: RUDN, 2008. 253 s.
10. Torokin A.A. Inzhenerno-tekhnicheskaya zashchita informatsii M.: Gelios ARV, 2005. 960 s.
11. Barsukov V.S. Bezopasnost': tekhnologii, sredstva, uslugi. M.: Kudits-Obraz, 2011. 500 s.
12. Katyurin Yu.F., Razumovskiy A.V., Spivak A.I. Zashchita informatsii tekhnicheskimi sredstvami. SPB.: NIU ITMO, 2012. – 418 s.
13. Atagimova E.I., Makarenko G.I., Fedichev A.V. Informatsionnaya bezopasnost'. Terminologicheskiy slovar' v opredeleniyakh deystvuyushchego zakonodatel'stva. M: FBU NTsPI pri Minyuste Rossii, 2015. 448 s.

4 Andrei Isaev, Ph.D., A.P., Financial University under the Government of Russia, Moscow, a.borisovich2010@yandex.ru
5 Antwan Alnadfa, RUDN, Moscow, antwan.tiger@gmail.com
6 Ivan Isaev, RUDN, Moscow