§7 МОДЕЛИ И МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Поначугин А.В., Одинцов И.В.

СИСТЕМА КОНТРОЛЯ ЗА НЕСАНКЦИОНИРОВАННОЙ ДЕЯТЕЛЬНОСТЬЮ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНОЙ СЕТИ

Аннотация: *В статье рассмотрены основные виды несанкционированной деятельности пользователей, анализ существующих подходов к защите информации в сети их архитектура и технические особенности реализации. Проведён подробный анализ системы контроля, которая призвана не только для мониторинга, но и для предотвращения деятельности злоумышленников в компьютерной системе организации. Так же демонстрируется построение системы безопасности как одного из главных органов организации и её обслуживание после внедрения на предприятии. Приведён список основных каналов утечки информации. Далее данная проблема раскрывается поэтапно, начиная от методов проникновения злоумышленников в компьютерную сеть организации, заканчивая действиями, которые должна произвести структура по защите данных. Выделена полная структура действий защитной системы. По итогам исследования можно будет сравнить существующие методы и службы, которые защищают компьютерную сеть от несанкционированного доступа, как из вне, так и внутри организации. Разработана пошаговая схема по созданию системы безопасности.Определен круг задач, которые она должна решать и проанализирована безопасность используемых сервисов.*

Ключевые слова: *конфиденциальная информация, несанкционированный доступ, компьютерная система, интернет, Cisco, компьютерные сети, безопасность, злоумышленник, нейросеть, уязвимость системы*

Abstract: *The article is devoted to the main types of users' unauthorized activity and analysis of existing approaches to the data security on the Internet, their design and technical implementation features. The authors of the article examine the control system designated not only to monitor but also to prevent malicious activity in corporate computer network. The authors also demonstrate the construction of the security system as one of the main organization departments and the system maintenance after it has been implemented. The authors provide the list of the main information leakage channels. After that, the authors unfold the problem step by step from the methods used*

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330

При цитировании этой статьи сноска на DOI обязательна

by intruders to get unauthorized access to the corporate computer network to the actions the data protection system must perform. The authors describe the full chain of actions to be completed by the security system. The results of the research allow to compare the existing methods and services protecting the computer network from unauthorized access both outside and inside the enterprise. The authors also develop the recurrence scheme for creating the security system, outline the scope of functions to be performed and analyze the security of the services used.
Keywords: *neuronet, system vulnerability, intruder, security, computer networks, Cisco, Internet, computer system, unauthorized access, confidential information*

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

В настоящее время работа многих организаций, компаний и обычных пользователей стала в значительной мере зависеть от надежного функционирования компьютерных систем. На компьютерные системы возлагается задача сохранения и обработки данных, которые зачастую имеют очень большую ценность. Получение несанкционированного доступа к ним, их уничтожение, изменение или разглашение, нелегальное использование ресурсов системы или приведение системы в недееспособное состояние – все это имеет крайне нежелательные последствия для владельцев этой информации. Поэтому проблема защиты компьютерных систем от злонамеренного вторжения является чрезвычайно актуальной.

В книге Энди Фокса и Дэвида Чемпена – Брандмауэры Cisco Secure PIX, авторы показывают, что в настоящее время огромное количество сетей объединено посредством Internet. И уследить за безопасной работой такой огромной системы достаточно сложно, но возможно с текущим уровнем технологий. Так же приводятся исследования, полученные - Институтом компьютерной безопасности, которые показывают, что у 70% организаций были взломаны системы сетевой защиты. Кроме того, 60% выявленных попыток взломов исходили из внутренних сетей организаций. [6].

В своем труде авторы рассказывают о брандмауэрах PIX, показывают все преимущества и недостатки данной системы защиты компьютерных сетей.

К этой же проблеме автор книги - Информационная безопасность компьютерных систем и сетей (КИС), В.Ф. Шаньгин, подходит именно со стороны корпоративных информационных сетей. Он показывает, как необходима КИС для любой организации, и выставляет её одним из главных рычагов бизнеса. Соответственно безопасность КИС, непосредственно влияет на развитие и благополучие предприятия. Автор вводит такое понятие как СИБ (система информационной безопасности). Она внедряется в уже существующую КИС, взаимодействуя с ней посредствам открытых стандартов и сетевых сервисов.

Не стоит забывать о том, что утечка любой информации может произойти даже из-за простейшего сбоя или заражения вирусом одного из компьютеров организации. [1]. Об этом очень подробно рассказывает Петр Ташков в книге – Защита компьютера на 100%: сбои, ошибки и вирусы. Данная книга написано простым и понятным языком. Автор описывает процессы сбоев системы, рассматривает диагностические методы и средства

DOI: 10.7256/2305-6061.2016.1.18330
При цитировании этой статьи сноска на DOI обязательна

необходимые для предотвращения и восстановления данных. [13].

Если авторы предыдущих книг рассказывают об оборудовании, сервисах, программных и аппаратных-средствах, и тем самым выстраивают всю защиту, отталкиваясь именно от этого, то Романец Ю.В. и Тимофеев П.А. в своем труде – Защита информации в компьютерных системах и сетях, возлагают всю систему защиты на плечи средствам и методам шифрования и криптографии. В книге представлено огромное количество всевозможных разновидностей алгоритмов и существующих систем. Отдельные главы посвящена вопросу хранения ключей и отечественному проекту КРИПТОН. [11].

Хоть и понятие "искусственные нейронные сети" начало формироваться ещё в 40-е годы XX века. Но именное в последние время стало всё больше развиваться в области информационной защите. Об этом в своей работе – Нейронные сети и нейроконтроллеры, рассказывает Бураков М.В.. Книга является учебным пособием, которое показывает основной принцип нейронов, а также, автор описывает работу сети, которая состоит из нейронов.

Все представленные здесь авторы имеют свою точку зрения решения проблемы компьютерной безопасности. Есть отличия в подходах к проблеме, в методах, даже в построении вопроса. Но, что их действительно объединяет, и с чего начинается любая из этих книг, то что с каждым днем значение информации становится только сильнее, и необходимость её защиты является едва ли не важнейшей задачей современности. С этим трудно не огласится, наблюдая лишь за тем, сколько в последние время IT-специалистов, и какое количество средств направляется именно в эту отрасль.

IT-специалист должен иметь некую базу знаний, которая ему понадобится для дальнейшей работы в этой области. И такой базой, должны стать высшие учебные заведения. Задача которых является подготовка высококлассного специалиста. [12].

Исходя из вышесказанного хочу предложить свою точку зрения по данной проблеме. Важным элементом обеспечение безопасности на современном этапе должно стать моделирование возможного поведения потенциальных нарушителей автоматизированными средствами. При данном подходе заранее предполагается, что нарушителем может являться и сотрудник компании, имеющие доступ к закрытой информации. Можно выделить несколько каналов утечки (рисунок 1).

Рисунок 1. Каналы утечки конфиденциальной информации

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330

При цитировании этой статьи сноска на DOI обязательна

Согласно данным последних исследований, наиболее «популярными» являются следующие каналы утечки информации:

1. Переносные запоминающие устройства.
2. Электронная почта.
3. Интернет (web-почта, форумы).
4. Интернет-пейджеры (ICQ, mail.ru agent).

Защита информации в компьютерных системах состоит в применении механизмов аутентификации и выявлении аномалий поведения пользователя или атак на компьютерную систему в реальном времени. [9]. Для этого предназначены системы выявления вторжений (intrusion detection systems – IDS). IDS обычно делят на системы, которые реагируют на уже известные атаки (системы выявления злоупотреблений) и системы выявления неизвестных ранее аномалий. [10]. Для выявления злоупотреблений обычно используются экспертные системы, работа которых основана на реализации набора известных заранее правил логического вывода. Работа существующих систем выявления злоупотреблений базируется на составлении шаблонов, или так называемых «подписей», известных атак. Затем с использованием экспертной системы в реальном времени производится анализ происходящих в системе событий и проверка их на схожесть с известными шаблонами. При этом последовательно выполняется серия проверок, позволяющих выявить возможную атаку. Защитные системы этого типа эффективны при выявлении известных типов атак. При некоторых отклонениях хода атаки от определенного шаблона возникают проблемы при их выявлении. Чтобы предотвратить подобные ситуации, необходимо поддерживать слишком большую базу данных по каждой известной атаке и ее вариациям.

Системы выявления аномалий, в отличие от экспертных систем, являются более гибкими. Они строятся на предположении, что все действия злоумышленника отличаются от поведения обычного пользователя и их можно рассматривать как аномалии поведения. Работе системы выявления аномалий предшествует период накопления информации, в течение которого составляется концепция нормальной активности системы или пользователя. Она считается эталоном, относительно которого оцениваются все последующие действия. На этом этапе обычно определяется перечень факторов, по которым можно вести наблюдение за деятельностью пользователей в системе. Теоретически, после составления шаблона нормального поведения, можно фиксировать все параметры системы (или их необходимую часть) и сигнализировать об отклонении этих параметров от обычных значений. Однако объем информации, генерируемой в больших системах (файлы аудита, поток данных в компьютерных сетях и тому подобная информация) может достигать нескольких мегабайт за час. Также постановка задачи – выявить аномальное поведение пользователя, отличающееся от обычного – плохо формализуется. Поэтому в последнее время все чаще предпринимаются попытки анализа аномального поведения пользователей на основе интеллектуальных методов обработки данных, в том числе с применением нейронных сетей [7].

Идея применения нейронных сетей в IDS, в частности в системах выявления аномалий, состоит в том, чтобы настроить сеть на некотором «обучающем» множестве значений

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330
При цитировании этой статьи сноска на DOI обязательна

вход-выход, которое характеризует поведение пользователя или системы. В качестве выхода сети может служить некоторый принятый коэффициент «нормальности поведения» или один из параметров системы. В процессе настройки нейронной сети выявляются и фиксируются скрытые закономерности, присутствующие во входных данных. После обучения такая нейронная сеть сможет анализировать поступающую информацию о работе пользователей и выявлять отклонения от их привычного поведения в системе. Если реальное поведение пользователя отличается от ожидаемого нейронной сетью, то делается вывод о наличии аномалии в системе и возможном нарушении ее безопасности. [5].

Для более полного и совершенного построения шаблона поведения пользователя предлагается, наряду с перечнем команд пользователя учитывать последовательность их выполнения. Это оправдано, поскольку пользователи отличаются друг от друга не только набором «излюбленных» команд, но и характерным порядком их использования. Информация о последовательности действий пользователя в компьютерной системе отображается в файлах аудита (журналах системных событий), формат и содержание которых зависит от операционной системы. Предлагаемый подход был реализован для операционной системы UNIX, а именно Free BSD, поскольку это одна из наиболее популярных и защищенных систем. [15].

Для каждого пользователя в системе строится нейронная сеть прямого распространения (настраиваемая по правилу обратного распространения ошибки) [2], которая обучается прогнозировать следующую команду данного пользователя на основе m предшествующих ей команд. Обученная таким образом нейросеть сможет моделировать поведение данного пользователя. Если реальное поведение пользователя в системе существенно отличается от «прогнозируемого» сетью поведения, значит с высокой вероятностью можно утверждать, что под данным именем в системе зарегистрировался посторонний пользователь.

После обучения нейронной сети на данных нескольких сеансов обучения с ее помощью можно анализировать деятельность пользователя в сети по информации файла аудита любого другого сеанса. В режиме тестирования на вход нейронной сети также предъявляется m команд, а полученное значение выхода сети сравнивается с реальной $(m+1)$-й командой. Если относительное количество правильно предсказанных команд на протяжении всего сеанса выше заданного порога, то поведение пользователя считается «нормальным», если нет – значит пользователь либо резко изменил свое поведение, либо под его именем работает другой пользователь. Поскольку пользователям свойственно изменять поведение с течением времени, то в процессе работы для обеспечения адаптации к их поведению, требуется периодически дополнять сеть новыми знаниями.

Такой подход обладает следующими преимуществами:

1. независимость от количества пользователей в системе, поскольку с каждым пользователем связывается отдельная нейронная сеть;
2. возможность выявления тонких закономерностей в поведении пользователя благодаря использованию информации не только о статистике выполнения команд, но и об их последовательности;

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330

При цитировании этой статьи сноска на DOI обязательна

3. возможность приспособления к изменяемому поведению пользователей;
4. возможность обучения сети на реальных данных без необходимости генерировать случайно или придумывать «аномальные» данные. [4].

На основании анализа существующей практики и проблематики, отражённой в научной литературе, можно сформировать следующие требования к современной компьютерной безопасности:

Безопасность компьютерных систем является одним из важнейших органов любой организации, поэтому её необходимо выстраивать исходя из всех даже вероятных угроз.

Изначально должно быть продумано место и роль система безопасности, а предприятии, затем необходимо моделирование с применением системного и факторного анализа. В результате проектирования и внедрения система безопасности должна решать такие задачи как:

– Выделение защищаемой области организации. Нужно определить, что конкретно нужно защитить и как это сделать. Для этого необходимо проводить постоянный мониторинг уязвимых мест компьютерной системы и разложить на составляющие все варианты, которые могут привезти к взлому безопасности.
– Отслеживание защищаемой области. После того как выбрана зона для защиты, необходимо заняться мониторингом этой области. Посмотреть, как система функционирует в состояние, когда ей не угрожает опасность. Здесь можно проследить какие устройства подключены и какой объем данных обрабатывается через сеть.
– Распределение прав доступа пользователей. Зачастую атаки происходят внутри сети, когда пользователь даже и не предполагает этого. Правильное распределение прав для сотрудников сможет оградить от этого.

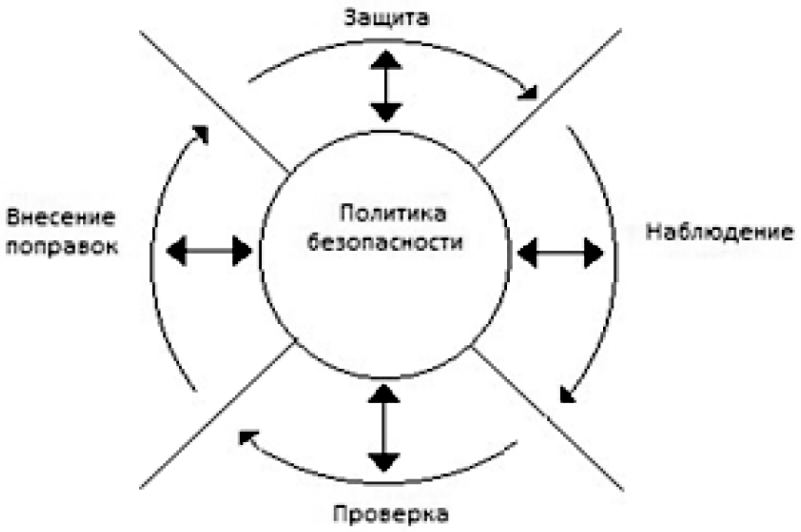

Рисунок 2. Схема обеспечения безопасности сети

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330
При цитировании этой статьи сноска на DOI обязательна

В обобщённом виде четыре части безопасности сети, которые должны присутствовать в системе защиты, для обеспечения наиболее высокой степени надежности компьютерной сети можно представить на схеме (рисунок 2). Все они работают согласованно, отталкиваясь друг от друга. Соответственно если одна из них будет повреждена, то и все остальные станут доступны для несанкционированного доступа к системе.

В заключении можно выделить компоненты, которые являются критически важными с технической стороны процесса обеспечения безопасности:

1. Аутентификация и идентификация. Некоторые специалисты называют данный сервис фундаментом программно-технических средств безопасности. [16].
2. Шифрование. Своеобразная стена, которая предназначена для перехвата и попадания несанкционированной информации в компьютерную сеть организации. [3].
3. Брандмауэры. Часто называемые в литературе межсетевыми экранами. Данная система способна разделять сеть на две или более частей и применить пакет операций, которые решают, как должна переходить информация от одной части в другую. [8].
4. Устранение ошибок системы. При создании и внедрении любой компьютерной системы, существуют «баги», которые не всегда удаётся обнаружить даже при всестороннем тестировании производительности и надёжности. Каждый маленький «баг» может являться потенциально уязвимостью в безопасности, и злоумышленники могут его использовать как способ проникновения в систему. [14].

После того как система безопасности настроена и внедрена на предприятии, необходимо помнить о том, что она постоянно нуждается в мониторинге ошибок, и проверки на новые угрозы. Так же необходимо следить, как за внешними, так и за внутренними атаками. Чем чаще будут проводиться технические проверки системы безопасности, её работоспособности и актуальности (как плановые, так и внеплановые) тем лучше. Но при этом необходимо придерживаться разумного компромисса в плане стоимости данных и стоимости систем их защиты. Только при выполнение всех выше перечисленных способов и технических средств, можно предотвратить несанкционированные атаки и обеспечить максимальную защиту вычислительной системы.

Что касается перспективы развития данной проблемы в целом, то мы наблюдаем постоянную эволюцию компьютерных систем, проникающих во все сферы жизнедеятельности человека. Параллельно этому развивается и не санкционированная деятельность, направленная на завладение той или оной информации путём проникновения через компьютерную сеть организаций. Соответственно возрастает её конечная ценность и необходимость защиты от несанкционированного доступа и хищения. Постоянно, руководствуюсь различными мотивами будет находиться тот, кто будет предпринимать попытки найти уязвимость в системе информационной безопасности. На данный момент существует огромное количество литературы, технических и программных средств, которые используют разные алгоритмы. Однако руководителям предприятий и специалистам по компьютерной безопасности не стоит думать о том, что, если одновременно

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330

При цитировании этой статьи сноска на DOI обязательна

использовать все доступные методы, безопасность системы будет максимальна. Выбор методов защиты должен быть индивидуальным для каждой конкретной компании, и модифицироваться с появлением новых угроз.

Библиография :

1. Алексанов А.К., Демчев И.А. Безопасность карточного бизнеса: бизнес-энциклопедия / ЦИПСиР; М., 2012. 277 с.
2. Болотова Ю.А., Спицын В.Г., Фомин А.Э. Применение модели иерархической временной памяти в распознавания изображений // Известия Томского политехнического университета. 2011. Т. 318. № 5. С. 60–63.
3. Брассар, Ж. Современная криптология / Ж. Брассар. М.:, 2013. 570 с.
4. Бураков, М.В. Нейронные сети и нейроконтроллеры: уч. пособие / М.В. Бураков. СПб: ГУАП, 2013. 284 с.
5. Гладких А.А., Дементьев В.Е. Базовые принципы информационной безопасности вычислительных систем: учебное пособие для студентов. Ульяновск: УлГТУ, 2009. 168 с.
6. Дэвид В. Чепмен, мл., Энди Фокс. Брандмауэры Cisco Secure PIX: Научно-популярное издание/ Издательский дом "Вильямс", 2003. 384 с.
7. Елизаров, А.И. Методика построения систем распознавания автомобильного номера / А.И. Елизаров. – Известия Томского политехнического университета, 2010. 118–121 с.
8. Зайцев А.П., Голубятников И.В. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е. М.: Машиностроение-1, 2006-260 с.
9. Менделевский И.Д. Атака через Internet / НПО «Мир и семья-95», 1997. 202 с.
10. Мигалова К.С., Поначугин А.В. Проблема безопасности электронных платежей. В сборнике: Перспективы развития науки Международная научно-практическая конференция. Отв. ред.: Сукиасян Асатур Альбертович. Уфа, 2015. С. 134-137.
11. Парошин А.А. Информационная безопасность: стандартизированные термины и понятия. Владивосток: Изд-во Дальневост. Ун-та, 2010. 216 с.
12. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных сетях / Под ред. В.Ф. Шаньгина. 2-е изд., перераб. и до. М.: Радио и связь, 2001. 376 с.
13. Степанов В.Г. Информационная безопасность: Учебно-методические материалы. М.:МИЭМП, 2005. 19 с.
14. Ташков П. Защита компьютера на 100%: сбои, ошибки и вирусы. Изд-во Питер, 2010. 288 с.
15. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. М.: ИД «ФОРУМ»; ИНФРА-М, 2008. 416 с.
16. Ясницкий Л.Н. Введение в искусственный интеллект: Учебное пособие для студ. высш. учеб. заведений / Л.Н. Ясницкий. М.: Издательский центр «Академия», 2010. 176 с.
17. Ященко В.В. Введение в криптографию / В.В. Ященко. М.: 2014. 705 с.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330
При цитировании этой статьи сноска на DOI обязательна

References:

1. Aleksanov A.K., Demchev I.A. Bezopasnost' kartochnogo biznesa: biznes-entsiklopediya / TsIPSiR; M., 2012. 277 s.
2. Bolotova Yu.A., Spitsyn V.G., Fomin A.E. Primenenie modeli ierarkhicheskoi vremennoi pamyati v raspoznavaniya izobrazhenii // Izvestiya Tomskogo politekhnicheskogo universiteta. 2011. T. 318. № 5. S. 60–63.
3. Brassar, Zh. Sovremennaya kriptologiya / Zh. Brassar. M.:, 2013. 570 s.
4. Burakov, M.V. Neironnye seti i neirokontrollery: uch. posobie / M.V. Burakov. SPb: GUAP, 2013. 284 s.
5. Gladkikh A.A., Dement'ev V.E. Bazovye printsipy informatsionnoi bezopasnosti vychislitel'nykh sistem: uchebnoe posobie dlya studentov. Ul'yanovsk: UlGTU, 2009. 168 s.
6. Devid V. Chepmen, ml., Endi Foks. Brandmauery Cisco Secure PIX: Nauchno-populyarnoe izdanie/ Izdatel'skii dom "Vil'yams", 2003. 384 s.
7. Elizarov, A.I. Metodika postroeniya sistem raspoznavaniya avtomobil'nogo nomera / A.I. Elizarov. – Izvestiya Tomskogo politekhnicheskogo universiteta, 2010. 118–121 s.
8. Zaitsev A.P., Golubyatnikov I.V. Programmno-apparatnye sredstva obespecheniya informatsionnoi bezopasnosti: Uchebnoe posobie. Izdanie 2-e. M.: Mashinostroenie-1, 2006-260 s.
9. Mendelevskii I.D. Ataka cherez Internet / NPO «Mir i sem'ya-95», 1997. 202 s.
10. Migalova K.S., Ponachugin A.V. Problema bezopasnosti elektronnykh platezhei. V sbornike: Perspektivy razvitiya nauki Mezhdunarodnaya nauchno-prakticheskaya konferentsiya. Otv. red.: Sukiasyan Asatur Al'bertovich. Ufa, 2015. S. 134-137.
11. Paroshin A.A. Informatsionnaya bezopasnost': standartizirovannye terminy i ponyatiya. Vladivostok: Izd-vo Dal'nevost. Un-ta, 2010. 216 s.
12. Romanets Yu.V., Timofeev P.A. Zashchita informatsii v komp'yuternykh setyakh / Pod red. V.F. Shan'gina. 2-e izd., pererab. i do. M.: Radio i svyaz', 2001. 376 s.
13. Stepanov V.G. Informatsionnaya bezopasnost': Uchebno-metodicheskie materialy. M.:MIEMP, 2005. 19 s.
14. Tashkov P. Zashchita komp'yutera na 100%: sboi, oshibki i virusy. Izd-vo Piter, 2010. 288 s.
15. Shan'gin V.F. Informatsionnaya bezopasnost' komp'yuternykh sistem i setei: uchebnoe posobie. M.: ID «FORUM»; INFRA-M, 2008. 416 s.
16. Yasnitskii L.N. Vvedenie v iskusstvennyi intellekt: Uchebnoe posobie dlya stud. vyssh. ucheb. zavedenii / L.N. Yasnitskii. M.: Izdatel'skii tsentr «Akademiya», 2010. 176 s.
17. Yashchenko V.V. Vvedenie v kriptografiyu / V.V. Yashchenko. M.: 2014. 705 c.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2016.1.18330

При цитировании этой статьи сноска на DOI обязательна