References

1. Shakurskiy M.V. Matematicheskiye modeli dvukhkomponentnykh invariantnykh steganograficheskikh sistem, ispol'zuyushchikh razlichnyye algoritmy svyazi vstraivayemykh signalov [Mathematical models of two-component invariant steganographic systems using various embedded signal coupling algorithms]. *Voprosy zashchity informatsii*, 2018, no. 2 (121), pp. 8–13. (In Russian).
2. Shakurskiy V.K., Shakurskiy M.V. *Szhimayushchiye otobrazheniya v invariantnykh preobrazovatelyakh i sistemakh steganografii* [Contraction Mapping in Invariant Transducers and Steganography Systems]. Samara: SNC RAN, 2014, 159 p. (In Russian).
3. Shakurskiy M.V. Formirovaniye konteynera dlya steganograficheskoy sistemy na osnove szhimayushchikh otobrazheniy [Forming a container for a steganographic system based on compressive mappings]. *Radiotekhnika*, 2015, no. 2, pp. 134–139. (In Russian).
4. Shakurskiy M.V., Shakurskiy V.K. Steganograficheskaya sistema na osnove szhimayushchikh otobrazheniy [Steganography system based on contraction mapping]. *Voprosy zashchity informatsii*, 2015, no. 2, pp. 74–78. (In Russian).
5. Shakurskiy M.V., Shakurskiy V.K. Otsenka stoykosti dvukhkomponentnoy steganograficheskoy sistemy [Evaluation of the durability of a two-component steganographic system]. *Uspekhi sovremennoy radioelektroniki*, 2015, no. 11, pp. 87–91. (In Russian).
6. Shakurskiy M.V., Shakurskiy V.K. Dvukhkanal'naya sistema sokrytiya informatsii s vzaimnym zashumleniyem kanalov [The dual-channel system of concealment of information with mutual channel noising]. *Radiotekhnika*, 2016, no. 2, pp. 96–99. (In Russian).
7. Patent RF. no. 2546307. Shakurskiy M.V., Shakurskiy V.K. *Ustrojstvo sokrytiya informacii* [Information hiding device]. No. 2014123943/08, decl. 10.06.2014, publ. 10.04.2015. Bul. no. 10.
8. Patent RF. no. 2546306. Shakurskiy M.V., Shakurskiy V.K. Sposob skrytoj peredachi informacii [The method of covert information transfer]. No. 2014123912/08, decl. 10.06.2014, publ. 10.04.2015. Bul. no. 10.
9. Patent RF. no. 167074. Shakurskiy M.V. Ustrojstvo sokrytiya informacii [Information hiding device]. No. 2016102913/08, decl. 28.01.2016, publ. 20.12.2016. Bul. no. №35.
10. Patent RF. no. 174362. Shakurskiy M.V., Shakurskiy V.K., Kozlovskijy V.N., Sorokin A.G. Ustrojstvo sokrytiya informacii [Information hiding device]. No. 2017109750, decl. 23.03.2017, publ. 11.10.2017. Bul. no. 29.

Received 20.01.2020

УДК 004.725.5

КОРПОРАТИВНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ: ПРОЦЕДУРЫ АУТЕНТИФИКАЦИИ И ИДЕНТИФИКАЦИИ

Василенко К.А.[1], Золкин А.Л.[2], Абрамов Н.В.[3], Курганов Д.О.[3]

[1] Владивостокский государственный институт экономики и сервиса, Владивосток, РФ

[2] Волжский государственный университет водного транспорта (Самарский филиал), Самара, РФ

[3] Дальневосточный федеральный университет, Владивосток, РФ

E-mail: k2857@mail.ru, alzolkin@list.ru, nikolay.abramov1990@mail.ru, kurganov_vl@mail.ru

В статье рассматриваются проблемы защиты персональных данных и информации от злоумышленников, способы аутентификации и идентификации в корпоративных сетях. Приведены различные методы аутентификации и идентификации в компьютерных сетях. Авторами проведен их сравнительный анализ, выделены особенности и недостатки в различных сферах использования, при этом проанализированы риски и возможный ущерб от нарушения конфиденциальности данных. Величина нарушений конфиденциальности, доступности и целостности информации с каждым годом все больше растет, вместе с тем растет и нанесенный ущерб, что вызывает необходимость у специалистов информационной безопасности все тщательней и углубленно вести анализ всех рисков незаконного доступа к информации, а затем прибегать к внедрению современных средств аутентификации, использовать новые методы шифрования, все чаще генерировать новые пароли доступа к системе. На сегодняшний день существует множество способов и методов аутентификации, но специфика их применения зависит от расположения хранилища информации и ее ценности. Между тем методы аутентификации не являются безупречными методами защиты, они также уязвимы, иногда многое зависит от навыков злоумышленников.

Ключевые слова: *корпоративные вычислительные сети, пароли, токены, аутентификация, идентификация, информационная безопасность, алгоритм действия*

Введение

Корпоративные вычислительные сети стали иметь немаловажное значение для аналитиков информационного рынка, поскольку в настоящее время прослеживается тенденция нарастающего развития угроз информационной безопасности. Это связано с распространением услуг мобильного банкинга и управления счетами, доступностью средств связи (смартфоны, коммуникаторы, планшеты) и персональных данных, накоплением электронных ресурсов, широким использованием облачных вычислений, стремлением российских компаний сохранить коммерческую тайну и нежеланием приглашать соответствующих специалистов, необходимостью доработки и настройки универсальных «коробочных» решений.

Аутентификация и идентификация как пути доступа к системе сети

Процедуры идентификации и аутентификации неразрывно связаны друг с другом. Они обязательно проводятся при каждом входе в систему или возобновлении работы без выхода из системы. Идентификация – это присвоение индивидуальных имен или номеров. Аутентификация – подтверждение подлинности идентификации субъекта системы. Авторизация – процедура предоставления определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

В данном случае под субъектом подразумевается любой участник безопасности, например учетная запись пользователя, созданная в службе каталога AD DS. Для того чтобы обеспечить управление и контроль над данными процедурами, дополнительно используются процессы администрирования и аудита.

Администрирование представляет собой процесс управления доступом к ресурсам системы. Этот процесс включает в себя:

– создание идентификатора (создание учетной записи пользователя) в системе;

– управление данными пользователя, применяемыми для его аутентификации (смена пароля, издание сертификата и т. п.);

– управление правами доступа к ресурсам системы.

Аудит – это процесс контроля доступа к ресурсам системы, включающий протоколирование действий при доступе к ресурсам системы для обеспечения возможности обнаружения попыток несанкционированных действий.

Для подтверждения своей подлинности необходимо предоставить некоторую секретную информацию. Существуют различные виды такой информации, которые можно обозначить одним термином – «фактор аутентификации».

Фактор аутентификации – определенный вид информации, предоставляемый субъектом системе при его аутентификации. Данная процедура может быть реализована с использованием одного или нескольких аутентификационных факторов. Например, у пользователя может быть запрошен пароль либо потребуется предоставить отпечаток пальца.

Однофакторная аутентификация – процесс, в котором используется только один тип аутентификационных факторов. Многофакторная аутентификация – процесс, в котором применяется несколько факторов. Например, при регистрации пользователь должен предоставить смарт-карту и пароль.

Выбор метода и средств аутентификации в сети и его рациональное использование

Наиболее распространено использование сочетания двух типов аутентификационных факторов. Характерным примером является работа с банкоматом. Нам требуется одновременно использовать карту с магнитной полосой и PIN-код. Многие руководители предприятий не уделяют должного внимания защите своих устройств и информации, которая находится на них. Подобная халатность зачастую приводит к финансовым убыткам в результате утечки информации. В настоящее время используют три основных метода однофакторной аутентификации: парольная аутентификация; биометрическая аутентификация; аутентификация с помощью токенов (смарт-карт) [2]. Также используются комбинации выше перечисленных методов аутентификации, называемые двухфакторной аутентификацией.

Парольная аутентификация – не самый надежный способ проверки подлинности пользователя. Как правило, люди используют пароли, которые легко запоминаются. Если же пароль достаточно надежный и состоит из большого количества символов, то пользователи часто пишут такие пароли на стикерах и приклеивают их к монитору, столу или внутренней части клавиатуры. Получить такой пароль не представляет сложности [3].

Политика информационной безопасности предлагает менять восьмизначный пароль минимум раз в месяц. Запоминать так часто случайным образом сгенерированный пароль довольно сложно. Забыв нужную последовательность символов, пользова-

тель обращается к администратору, который присылает пароль. Данная процедура также небезопасна, потому что пароль можно перехватить по сети. Чтобы этого не произошло, сообщение с паролем нужно зашифровать или передавать по защищенному каналу. Все это ведет к дополнительным затратам. Во многих фирмах звонка администратору недостаточно для получения пароля. Необходима служебная записка или личный визит администратора, что, в свою очередь, также ведет к потере времени и финансовым затратам. Можно сделать вывод, что метод парольной аутентификации неэффективен в силу «человеческого фактора» [4].

В последнее время широкое распространение получили так называемые токены, USB- ключи или смарт-карты. Данный метод аутентификации может реализовываться с помощью: генерации одноразовых паролей, хранения в памяти устройства паролей, ключей шифрования, цифровых сертификатов. Помимо пароля пользователю необходимо воспользоваться устройством. В зависимости от потребностей внешний вид аппаратных средств может быть разный, для контроля доступа к персональным компьютерам или помещениям используется смарт-карта со встроенной RFID-меткой [5].

Наиболее эффективным в плане защищенности будет использование смарт-карт и USB-ключей, такой идентификатор тяжелее украсть, и его потеря откроется быстрее, чем кража пароля. Помимо этого, в таких устройствах используется двухфакторная аутентификация, что значительно повышает надежность системы, но следует учитывать и возможность подмены сервера аутентификации [6].

В корпоративных вычислительных сетях биометрическими системами стали пользоваться относительно недавно. Это достаточно дорогие системы, поэтому немногие организации могут приобрести и администрировать их.

Биометрическая аутентификация – надежный способ аутентификации, но не исключены ситуации, при которых данный идентификатор может быть украден или испорчен. Отпечатки носителя идентификатора можно украсть, например, со стакана, дверной ручки и т. д.

Алгоритм действия биометрической аутентификации [7].

1. Биометрическая система записывает образец биометрических черт пользователя с помощью считывателя.

2. С помощью программного алгоритма извлекаются индивидуальные черты.

3. Вместе с другими идентификаторами в базе данных сохраняются и черты.

4. Для аутентификации необходимо предъявить оригинал биометрической черты, который с помощью алгоритма сопоставления сравнивается с данными из базы данных.

5. Система открывает доступ, только если рейтинг соответствия превысил выставленный ранее порог.

Биометрическая аутентификация построена на принципе считывания анатомических и поведенческих особенностей человека: отпечатков пальцев (ладони); сканирования сетчатки глаза (радужной оболочки глаза); геометрии и термограммы лица; по голосу; по клавиатурному подчерку. Аутентификация по отпечатку пальца происходит с помощью специальных сканеров. Аутентификация по сетчатке и радужной оболочке считается наиболее отказоустойчивой с минимальными ошибками, но долгое время не использовалась в силу своей дороговизны и сложности [8].

Одним из наиболее надежных способов аутентификации является сканирование радужной оболочки глаза. В качестве источника для идентификации используется ткань глаза, которая генетически у всех индивидуальная. В ходе исследований учеными-медиками было установлено, что при заболеваниях глаза на радужной оболочке образуются пигментные пятна. Чтобы решить данную проблему, в сканерах используют черно-белые изображения. Фокусировка глаза происходит с помощью регистрирующей аппаратуры на расстоянии до одного метра. Далее аппарат формирует примерно 250 точек идентификации на роговице. Аутентификация происходит путем сравнения отсканированных точек с эталоном, который хранится в базе.

Аутентификация по геометрии и термограмме лица основана на распознании человека по его внешним характеристикам (форме носа, черепа, чертам лица) и разделяется на две категории: 2D- и 3D-распознание лица. Наиболее эффективным методом считается 3D-распознание лица. Аутентификация по термограмме лица основана на сканировании инфракрасным лучом кровеносных сосудов на лице и создании термокарты. Главное преимущество данного метода заключается в том, что система сосудов не зависит от температуры тела и остается неизменной, даже если были применены методы конспирации или сделана пластическая операция.

Аутентификация по голосу происходит путем сравнения голоса говорящего с данными из базы. Существует несколько методов аутентификации: текстонезависимая; текстозависимая по статической парольной фразе; текстозависимая по динамической парольной фразе, а также

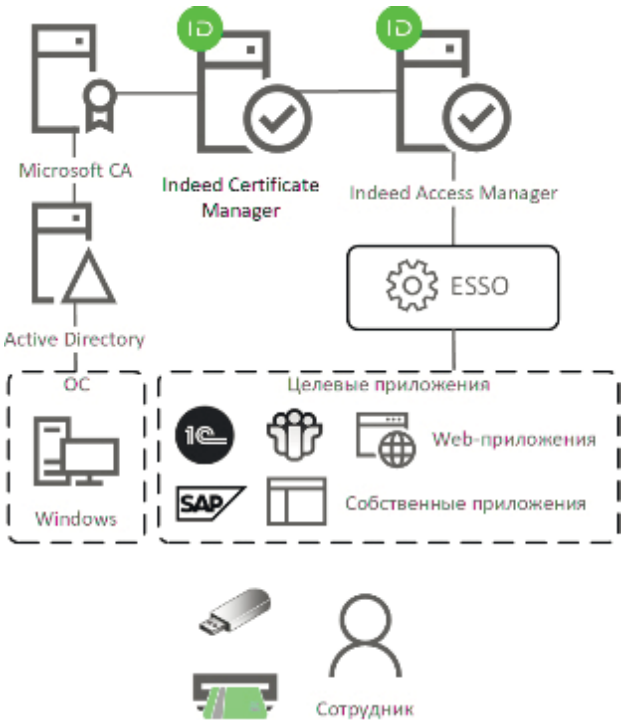

Рисунок. Двухфакторная аутентификация в операционных системах

по рукописному и клавиатурному подчерку. При разработке систем аутентификации по рукописному подчерку необходимо учитывать внешние факторы, влияющие на состояние человека. Поэтому допускается большая погрешность, что увеличивает вероятность взлома или подделки идентификатора.

Хранение биометрических данных в соответствии с Федеральным законом «О персональных данных» в соответствующей базе данных достаточно дорого, что также является минусом.

Двухфакторная аутентификация – это совокупность двух или даже трех факторов, чаще всего это пары: что-то знать и что-то иметь; что-то знать и кем-то являться. Пример работы данного метода представлен на рисунке. С точки зрения безопасности такой метод более эффективен, чем использование одиночных методов аутентификации.

Обеспечение единоличного доступа пользователя к его учетной записи, притом что ключ может быть известен кому-то еще из злоумышленников, может гарантировать именно двухфакторная аутентификация. В данном случае она выступает как дополнительная стадия безопасности ID. Определив перечень устройств, которым доверяет пользователь, двухфакторная аутентификация может вести синхронизацию между данными устройствами по одной учетной записи, обеспечив безопасный вход в каждое из них. Например, введение пароля и многозначного кода в некоторых гаджетах являются основными двумя видами информации при первом входе на новой технике.

При этом отображение как пароля, так и кода будет автоматически воспроизводиться на включенной в перечень доверенной технике. Как только будет введен код, перечень доверенных устройств будет пополнен новой техникой. Если вход окажется выполненным, то введение заново нового кода подтверждения уже не понадобится, его запрос на устройстве будет отсутствовать, пока пользователь не произведет выход либо данные в технике не будут отформатированы, либо пользователю потребуется внезапная смена пароля. При этом возможен вход через Internet, однако при данных условиях стоит признать браузер достоверным и доверенным, в результате чего при следующем входе с технического устройства запрос на код подтверждения безопасности не появится.

Для того чтобы устройство признать доверенным, это должна быть такая техника, у которой для пользователя должны быть идентифицированы и известны все факты ее принадлежности, в чьих интересах она работает. Однако главное направление данного устройства при свойстве доверенности – это возможность идентификации личности, например, путем отображения и установления кода входного подтверждения при эксплуатации другой доверенной техники или браузера [9].

Также стоит обратить внимание на значимость номера телефона, который стоит признавать доверенным. Этот номер должен выполнять функции получения и отображения специальных кодов подтверждения, при этом использовать текстовые сообщения, различные рассылки идентификационных данных, автоматические телефонные вызовы. Двухфакторная аутентификация предусматривает подтверждение как минимум одного достоверного и доверенного номера телефона, только тогда будет сформирован путь доступа к данным.

Кроме того, наличие дополнительного доверенного номера телефона, к которому пользователь будет иметь доступ, является также применимым вариантом аутентификации в рамках безопасности. Это может быть как домашний телефон, так и телефон друзей и близких, членов семьи, то есть лиц, которым пользователь доверяет. Обычно дополнительный доверительный номер используется при временном отсутствии доступа к основному номеру или вообще ко всей доверенной синхронизированной технике.

Сам код подтверждения можно определить как временный шифр, который с целью входа отправляет пользователь на доверенную технику либо на доверенный телефонный номер, при этом вход должен быть первичным, с использованием идентификатора ID он также может быть осуществлен не на самом устройстве, а через браузер.

VPN-сети и Internet-ресурсы различных видов чаще всего применяют для своих путей доступа такие методы, как смарт-карты, USB-ключи, SMS-сообщения, email-сообщения, в которых присутствует наличие специального кода аутентификации.

Также в корпоративном секторе иногда используются генераторы кодов (в виде брелока с кнопкой и дисплеем небольшого размера), технология SecureID и некоторые другие специфические методы, характерные в основном для данного сектора. Есть и менее современные интерпретации: например, так называемые TAN-пароли (Transaction Authentication Number – аутентификационный номер транзакции). К примеру, данный метод используется при обслуживании клиентов какого-нибудь не самого прогрессивного банка: при подключении интернет-банкинга клиенту выдается документ с заранее сформированным списком одноразовых паролей, которые вводятся один за другим при каждом входе в систему и/или совершении транзакции [10]. При этом банковская карта и PIN тоже формируют систему двухфакторной аутентификации: карточка – «ключ», которым вы владеете, а PIN-код к ней – «ключ», который пользователь запоминает.

С тем существует обязательная зависимость между специальным клиентским программным обеспечением и многими техническими продуктами, имеющими функцию многофакторной аутентификации. Чтобы войти в сеть, программистами были разработаны специальные инсталляционные программные продукты, позволяющие использовать смарт-карту либо токен с условием установки на персональный компьютер нескольких подобных программ. Данные пакеты программ ведут ревизионный контроль и проверку на наличие конфликтов между приложениями и техническими устройствами, а также осуществлению специальные обновлений [11]. Но чаще всего доступ к устройству производится при использовании веб-страниц. С другими программными решениями многофакторной аутентификации, такими как «виртуальные» токены или некоторые аппаратные токены, ни одно ПО не может быть установлено непосредственными пользователями.

Заключение

Выбор средств аутентификации и других дополнительных мер защиты важно основывать на анализе потенциальных потерь в той или иной ситуации. Если анализ рисков показывает, что возможный ущерб от нарушения конфиденциальности, целостности или доступности информации достаточно велик, то полагаться на пароли в этих ситуациях – удовольствие гораздо более дорогое, чем закупка и внедрение современных средств двухфакторной аутентификации. Несмотря на большое многообразие методов аутентификации, всегда присутствует хотя бы маленький процент уязвимости. Обусловлено это непрерывным и стихийным явлением развития информационных технологий, модернизацией техники и компьютеризацией данных.

Литература

1. Береза Н.В. Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона. 2012. № 2. URL: https://ivdon.ru/ru/magazine/archive/n2y2012/758 (дата обращения: 22.12.2019).
2. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2017. 255 с.
3. Панкратов С.А. Использование графической информации для защиты программного и информационного обеспечения // Инженерный вестник Дона. 2012. № 2. URL: https://ivdon.ru/ru/magazine/archive/n2y20 12/792 (дата обращения: 22.12.2019).
4. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. М.: Лори, 2016. 480 с.
5. Аладышев О.С., Овсянников А.П, Шабанов Б.М. Развитие корпоративной сети Межведомственного суперкомпьютерного центра. URL: https://vbakanov.ru/metods/1441 (дата обращения: 22.12.2019).
6. Гайдук А.Р. Теория и методы аналитического синтеза систем автоматического управления (полиномиальный подход). М.: Физматлит, 2017. 264 с.
7. Khalil H.K. Nonlinear Systems. 3rd ed. Upper Saddle River: Prentice Hall, 2016. 766 p. URL: https://en.bookfi.net/book/1417228 (дата обращения: 22.12.2019).
8. Melin P., Castillo O. Modeling, Simulation and Control of Non-linear Dynamical Systems:

An Intelligent Approach Using Soft Computing and Fractal Theory. Boca Raton: Taylor & Francis, 2017. 265 p.
9. Смирнов А.В. Руководство по захвату сетевого трафика. URL: https://blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-network-cards (дата обращения: 22.12.2019).
10. Perlman R. Interconnections: Bridges & Routers. Boston: Addison-Wesley, 2016. 245 p.
11. Oggerino C. High Availability Network Fundamentals. Indianapolis: Cisco Press, 2017. 327 p.

Получено 04.02.2020

Василенко Константин Александрович, преподаватель Колледжа сервиса и дизайна Владивостокского государственного университета экономики и сервиса. 690092, Российская Федерация, Приморский край, г. Владивосток, ул. Добровольского, 20. Тел. +7 964 453-06-36. E-mail: k2857@mail.ru

Золкин Александр Леонидович, к.т.н., преподаватель кафедры естественнонаучных и общепрофессиональных дисциплин Волжского государственного университета водного транспорта (Самарский филиал). 443099, Российская Федерация, г. Самара, ул. Молодогвардейская, 62-64. Тел. +7 960 825-68-49. E-mail: alzolkin@list.ru

Абрамов Николай Викторович, студент Дальневосточного федерального университета (ДВФУ). 690920, Российская Федерация, Приморский край, г. Владивосток, ул. Суханова, 8. Тел. +7 914 373-91-16. E-mail: nikolay.abramov1990@mail.ru

Курганов Даниил Олегович, студент ДВФУ. 690920, Российская Федерация, Приморский край, г. Владивосток, ул. Суханова, 8. Тел. +7 999 059-37-74. E-mail: kurganov_vl@mail.ru

ENTERPRISE DATA PROCESSING NETWORKS: AUTHENTICATION AND IDENTIFICATION PROCEDURES

Vasilenko K.A.[1], Zolkin A.L.[2], Abramov N.V.[3], Kurganov D.O.[3]
[1] Vladivostok State University of Economics and Service, Vladivostok, Russian Federation
[2] Volga State University of Water Transport (Samara branch), Samara, Russian Federation
[3] Far Eastern Federal University, Vladivostok, Russian Federation
E-mail: k2857@mail.ru, alzolkin@list.ru, nikolay.abramov1990@mail.ru, kurganov_vl@mail.ru

This article is dedicated to the problem of personal data and information protection from intruders, as well as to methods of authentication and identification in the enterprise data processing networks. Different methods of authentication and identification in data processing networks are given in the article. The authors have conducted the comparative analysis of these methods, have highlighted the features and weaknesses of these methods in different fields of application. In addition to the above the authors have conducted the risks analysis and analyzed the possible losses in case of confidentiality compromise. Every year, the amount of violations in data confidentiality, availability and integrity is growing as well as the amount of caused losses. These facts make cyber security specialists conduct more careful and deep analyses of all risks of unauthorized access to the information and then to introduce modern authentication means, use new coding methods and increase the frequency of generation of the new system access passwords. Today, there are many authentication means and methods, but the specifics of their application depend on the location of the information storage and its value. Meanwhile, the authentication methods are not flawless methods of protection, they are also vulnerable and success of their hack depends on the skills of the intruders.

Keywords: *enterprise data processing networks, passwords, tokens, authentication, identification, information safety, algorithm*

DOI: 10.18469/ikt.2020.18.1.10

Vasilenko Konstantin Alexandrovich, Service and Design College of the Vladivostok State University of Economics and Service, 20, Dobrovolskogo Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Heighest Category Lecturer. Tel. +7 964 453-06-36. E-mail: k2857@mail.ru

Zolkin Alexander Leonidovich, Volga State University of Water Transport (Samara branch), 62-64, Molodogvardeyskaya Street, Samara, 443099, Russian Federation; PhD in Technical Science, Lecturer of Natural-Science and General Professional Disciplines Sub-Faculty. Tel. +7 960 825-68-49. E-mail: alzolkin@list.ru

Abramov Nikolai Viktorovich, Far Eastern Federal University, 8, Sukhanova Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Student. Tel. +7 914 373-91-16. E-mail: nikolay.abramov1990@mail.ru

Kurganov Daniil Olegovich, Far Eastern Federal University, 8, Sukhanova Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Student. Tel. +7 999 059-37-74. E-mail: kurganov_vl@mail.ru

References

1. Bereza N.V. Sovremennie tendentsii razvitiya mirovogo i rossiyskogo rinka informatsionnikh uslug [Current trends in the development of the global and Russian markets of information services]. *Inzhenerniy vestnik Dona*, 2012, № 2. URL: https://ivdon.ru/ru/magazine/archive/n2y2012/758 (accessed: 22.12.2019). (In Russian).
2. Bondarev V.V. *Vvedenie v informatsionnuyu bezopasnost avtomatizirovannikh sistem: uchebnoe posobie* [Introduction to Information Security of Automated System: Study Guide]. Moscow: MGTU im. N.E. Baumana, 2017, 255 p. (In Russian).
3. Pankratov S.A. Ispolzovanie graficheskoy informatsii dlya zaschiti progrmanogo i informatsionnogo obespecheniya [Use of graphical information for protection of the software and data intelligence]. *Inzhenerniy vestnik Dona*, 2012, № 2. URL: https://ivdon.ru/ru/magazine/archive/n2y2012/792 (accessed: 22.12.2019). (In Russian).
4. Ed Willson. *Monitoring i analiz setey. Metodi viyavleniya neispravnostey* [Network Monitoring and Analysis. Fault Identification Methods]. Moscow: Lori, 2016, 480 p. (In Russian).
5. Aladishev O.S., Ovsyannikov A.P., Shabanov B.M. *Razvitie korporativnoy seti Mezhvedomstvennogo superkomputernogo centra* [Development of enterprise network of Interagency supercomputer center] URL: https://vbakanov.ru/metods/1441 (accessed: 22.12.2019). (In Russian).
6. Gaiduk A.R. *Teoriya i metody analiticheskogo sinteza sistem avtomaticheskogo upravleniya: (polinominalnii podhod)* [Theory and Methods of Analytical Synthesis of Automatic Control Systems (Polynomial Approach): Monograph]. Moscow: Fizmatlit, 2017, 264 p. (In Russian).
7. Khalil H.K. *Nonlinear Systems. 3rd ed.* Upper Saddle River: Prentice Hall, 2016, 766 p. URL: https://en.bookfi.net/book/1417228 (accessed: 22.12.2019).
8. Melin P., Castillo O. *Modeling, Simulation and Control of Non-linear Dynamical Systems: An Intelligent Approach Using Soft Computing and Fractal Theory*. Boca Raton: Taylor & Francis, 2017, 265 p.
9. Smirnov A.V. *Rukovodstvo po zahvatu setevogo trafika* [Network Traffic Capture Guide]. URL: https://blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-network-cards (accessed: 22.12.2019). (In Russian).
10. Perlman R. *Interconnections: Bridges & Routers*. Boston: Addison-Wesley, 2016, 245 p.
11. Oggerino C. *High Availability Network Fundamentals*. Indianapolis: Cisco Press, 2017, 327 p.

Received 04.02.2020