УДК 004.056.5

05.00.00 Технические науки

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЭКОНОМИЧЕСКОЙ СФЕРЕ

Бабенков Игорь Михайлович
РИНЦ SPIN-код=2824-0560
начальник информационно-технического отдела
НЧОУ ВО Кубанский институт информзащиты, Краснодар, Россия
350010, г.Краснодар, ул. Зиповская, 5 лит.Б
kiiz@bk.ru

Параскевов Александр Владимирович
РИНЦ SPIN-код= 2792-3483
старший преподаватель кафедры компьютерных технологий и систем
Кубанский государственный аграрный университет, Краснодар, Россия
350044, г.Краснодар, ул.Калинина, 13
paraskevov.alexander@gmail.com

Девять из десяти диверсий совершаются людьми, так или иначе связанными с информационными технологиями. По мнению экспертов компании InfoWatch, разработчика систем защиты конфиденциальной информации от инсайдеров, причина такой профессиональной принадлежности кроется в психологических особенностях этих служащих. Подробнее разобраться в проблеме позволит пара примеров из жизни, наиболее ярко иллюстрирующие типичные черты характера профессионалов в информационной среде. Причем если первый рассказчик не стал скрывать своего имени, то второй решил остаться неизвестным. Глубокая психологическая подоплека акта диверсии часто приводит к тому, что рассерженный служащий угрожает начальству или сослуживцам, например, по электронной почте. Иногда он даже делится своими мыслями с кем-то из коллег. Другими словами, информация о готовящейся диверсии есть не только у злоумышленника. Аналитики подсчитали, что в 31% случаев сведениями о планах диверсанта располагают другие люди. Из них 64% — коллеги, 21% — друзья, 14% — члены семьи, а еще 14% — сообщники. Также удалось установить, что 62% корпоративных диверсантов продумывают свои действия заблаговременно. В 47% случаев они совершают подготовительные действия (например, кража резервных копий конфиденциальных данных). В 27% — конструируют и проверяют механизм будущей атаки (готовят логическую бомбу в корпоративной сети, дополнительные скрытые входы в систему и т.д). При этом в 37% случаев активность сотрудников можно заметить: из этого количества 67% подготовительных

UDC 004.056.5

Technical sciences

MEANS AND METHODS OF INFORMATION SECURITY IN THE ECONOMIC SPHERE

Babenkov Igor Mihaylovich
SPIN code =2824-0560
chief of the Information and technology division
Kuban institute of information protection, Krasnodar, Russia
350010, Krasnodar, Zipovskaja, 5 lit.B
kiiz@bk.ru

Paraskevov Alexander Vladimirovich
SPIN code = 2792-3483
senior lecturer of the Department of computer technologies and systems
Kuban State Agrarian University, Krasnodar, Russia
350044, Krasnodar, Kalinina, 13
paraskevov.alexander@gmail.com

People commit nine out of ten acts of sabotage, one way or another associated with information technologies. According to experts at InfoWatch, developer of systems to protect confidential information from insiders, the reason for this profession lies in the psychological characteristics of these employees. To understand the problem let a couple of real-life examples illustrate the typical traits of professionals in the information environment. In addition, if the first teller did not hide his name, the latter decided to remain anonymous. Deep psychological background of the act of sabotage often leads to the fact that a disgruntled employee threatens boss or coworkers, for example, by e-mail. Sometimes he even shares his thoughts with someone from colleagues. In other words, it is not only the attacker, who knows the information about the planned diversion. Analysts estimate, that in 31% of cases, other people have the information about the plans of the saboteur. Of these, 64% are colleagues, 21% are friends, 14% — family members, and another 14% are allies. In addition, we were able to establish that 62% of corporate saboteurs think about their actions in advance. In 47% of cases, they commit preparatory acts (e.g., theft of confidential data backups). 27% — design and test of the future mechanism of the attack (preparing a logic bomb for the corporate network, additional hidden inputs to the system, etc.). Whilst in 37% of cases of the activity of employees, you may notice: 67% of the preparatory action may be visible online, 11% are visible offline, 22% — both at once

действий заметны в режиме online, 11% — offline, 22% — обоих сразу

Ключевые слова: IT ДИВЕРСИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОРПОРАТИВНАЯ СРЕДА, СЕТЕВЫЕ ТЕХНОЛОГИИ, АУДИТ БЕЗОПАСНОСТИ

Keywords: IT SABOTAGE, INFORMATION SECURITY, ENTERPRISE ENVIRONMENT, NETWORK TECHNOLOGY, SECURITY AUDIT

Первостепенной целью информационной безопасности является обеспечение конфиденциальности. Утечка информации может привести к необратимым последствиям. Все юридические лица обязаны использовать технические средства, предназначенные для защиты информации. Огромную помощь в этом оказывают средства шифрования информации. Люди, нарушившие закон, стоящие на учете в психоневрологическом или наркологическом диспансере, не могут быть допущены к работе с конфиденциальной информацией. Работники, допущенные к подобной информации, обязаны дать обязательство в письменном виде о её неразглашении. Причиной возникновения отклонений в соблюдении информационной безопасности является нарушение движения информационных потоков или ошибки в системе доступа.

Наиболее часто встречающиеся примеры нарушения доступа к информации:

– ошибки администрирования;

– неправильное формирование групп пользователей и определение прав их доступа;

–отсутствие политики формирования паролей пользователей;

–ошибки в формировании итоговых и агрегированных отчетов, доступа к ним;

–наличие открытого канала доступа для сторонних лиц;

– ошибки проектирования информационной системы;

–использование слабозащищенной среды для разработки информационной системы, где доступ к информации можно получить не

через интерфейс программы, который требует пароля, а напрямую, читая из таблиц баз данных;

– ошибки алгоритмов доступа к данным;

– небрежность в разработке системы защиты;

– небрежность пользователей в вопросах информационной безопасности;

– нарушение хранения паролей для доступа в информационную систему;

– сохранение закрытого соединения после окончания работы, данное нарушение делает бессмысленным большинство других требований системы безопасности;

– нерегламентированное обсуждение зарытой информации;

– умышленный взлом системы.

При правильном построении системы информационной безопасности нерегламентированные изменения могут быть зарегистрированы и выявлены в процессе работы. Кроме того, существуют дополнительные механизмы защиты от них, такие как электронная подпись, благодаря чему общее количество данных нарушений меньше, чем нарушений доступа на просмотр информации, хотя их последствия более серьезны.

Причины, приводящие к нарушениям записи информации в системе, можно сгруппировать следующим образом:

– ошибки программирования;

– ошибки ввода;

– технические сбои;

– умышленные нарушения в системе.

Причины утраты работоспособности и производительности кроются в механизмах самой системы, в ее способности совершать различные

действия. Ущерб от подобных нарушений зависит от степени частичного снижения или полной потери работоспособности.

Наиболее распространенной причиной нарушений в работе информационных систем являются ошибки их пользователей – непреднамеренные ошибки сотрудников организации. Как правило, данные нарушения не приводят к большому ущербу, хотя возможны и исключения. Современные механизмы контроля и мониторинга позволяют почти полностью исключить этот тип нарушений. Однако из-за большого количества разновидностей ошибок создание системы, полностью исключающей их появление, как правило, невозможно или связано с неоправданными затратами.

Другой случай – это преднамеренные действия сотрудников, нарушения, которые являются самыми сложными для предотвращения. Сотрудник организации, как правило, хорошо ориентируется во внутренних процессах и системах. Часто он знает о механизмах безопасности и, что более опасно, об их отсутствии в определенных модулях системы. У него есть время и возможность смоделировать и протестировать свои действия, оценить последствия.

Причинами, побудившими сотрудников к умышленному нарушению информационной безопасности, являются:

– обида на действия менеджеров, как правило, связанная с конфликтами или увольнением сотрудника;

– попытка дополнительного заработка;

– попытка хищения денег из организации;

– попытка создания зависимости организации от конкретного сотрудника;

– карьерная борьба.

В качестве мер противостояния нарушениям данного типа наиболее эффективны социально-экономические меры, разграничение доступа и

мониторинг действий пользователей. Еще одна группа причин нарушений в работе информационных систем – действия сторонних лиц криминального характера.

Система информационной безопасности тесно связана с техническими проблемами, решение которых может потребовать значительных сроков и ресурсов, что может привести к экономической нецелесообразности использования рассматриваемых механизмов.

Обеспечение информационной безопасности достигается системой мер, направленных[8]:

– на предупреждение угроз. Предупреждение угроз – это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

– на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

– на обнаружение угроз;

– на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

– на ликвидацию последствий угроз и преступных действий и восстановление системы.

Основной концепцией обеспечения ИБ объектов является комплексный подход, который основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных [7]. Оценка эффективности может быть проведена по кривой роста относительного уровня обеспечения безопасности от наращивания средств контроля доступа (см. рис.1).

Рисунок 1 – Кривая роста относительного уровня обеспечения безопасности

Для гарантии того, чтобы только зарегистрированные в автоматизированной системе пользователи могли включить компьютер (загрузить операционную систему) и получить доступ к его ресурсам, каждый доступ к данным в защищенной АС осуществляется в три этапа: идентификация – аутентификация – авторизация [6,7]. Идентификация – присвоение субъектам и объектам доступа зарегистрированного имени, персонального идентификационного номера (PIN-кода), или идентификатора, а также сравнение (отождествление) предъявляемого идентификатора с перечнем присвоенных идентификаторов. Основываясь на идентификаторах, система защиты «понимает», кто из пользователей в данный момент работает на ПЭВМ или пытается включить компьютер (осуществить вход в систему). Аутентификация определяется как проверка принадлежности субъекту доступа предъявленного им идентификатора, либо как подтверждение подлинности субъекта. Авторизация – предоставление пользователю полномочий в соответствии с политикой безопасности, установленной в компьютерной системе. Процедуры идентификации и аутентификации в защищенной системе осуществляются

посредством специальных программных средств. Процедура идентификации производится при включении компьютера и заключается в том, что сотрудник «представляется» компьютерной системе. Далее пользователь должен убедить систему в том, что он действительно тот, кем представился.

Современные программно-аппаратные средства идентификации и аутентификации по виду идентификационных признаков можно разделить на электронные, биометрические и комбинированные. В отдельную подгруппу в связи с их специфическим применением можно выделить системы одноразовых паролей, входящие в состав электронных (см. рис.2).

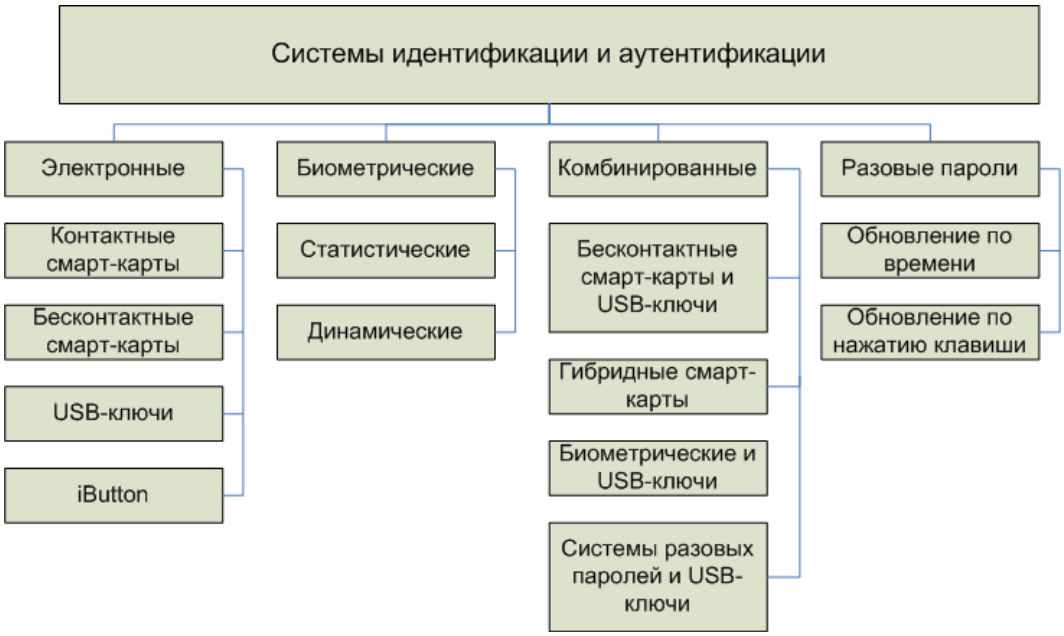

Рисунок 2 – Классификация программно-аппаратных систем идентификации и аутентификации

В электронных системах идентификационные признаки представляются в виде кода, хранящегося в памяти идентификатора (носителя). Идентификаторы в этом случае бывают следующие: контактные смарт-карты; бесконтактные смарт-карты; USB-ключи (USB-token); iButton.

В комбинированных системах используется одновременно несколько признаков, причем они могу принадлежать как системам одного класса, так и разным. В состав электронных систем идентификации и аутентификации входят контактные и бесконтактные смарт-карты и USB-token [2]. Бесконтактные смарт-карты разделяются на идентификаторы Proximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации (см. табл. 1).

Таблица 1 – Радиочастотные идентификаторы

Характеристика	Proximity	Смарт-карты	
		ISO/IEC 14443	ISO/IEC 15693
Частота радиоканала	125 кГц	13,56 МГц	13,56 МГц
Дистанция чтения	До 1м	До 10см	До 1м
Встроенные типы чипов	Микросхема памяти, микросхема с жесткой логикой	Микросхема памяти, микросхема с жесткой логикой, процессор	Микросхема памяти, микросхема с жесткой логикой
Функции памяти	Только чтение	Чтение-запись	Чтение-запись
Емкость памяти	8–256 байт	64 байт – 64 кбайт	256 байт – 2 кбайт
Алгоритмы шифрования и аутентификации	Нет	Технология MIRAGE, DES, 3DES, AES, RSA, ECC	DES, 3DES
Механизм антиколлизии	Опционально	Есть	Есть

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счет сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические. Статическая биометрия основывается на данных, полученных из измерений анатомических особенностей человека. Динамическая основывается на анализе действий.

Основными компонентами бесконтактных устройств являются чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64 разрядные серийные номера.

Системы идентификации на базе Proximity криптографически не защищены, за исключением специальных заказных систем.

USB-ключи работают с USB-портом компьютера. Изготавливаются в виде брелоков. Каждый ключ имеет прошиваемый 32/64 разрядный серийный номер.

Аутентификация в защищенных автоматизированных системах может осуществляться несколькими методами [2,3]:

• парольная аутентификация;

• на основе биометрических измерений;

• с использованием физических носителей аутентифицирующей информации.

Наиболее простым и дешевым способом аутентификации личности в АИС является ввод пароля (трудно представить себе компьютер без клавиатуры). Однако существование большого количества различных по механизму действия атак на систему парольной защиты делает ее уязвимой перед подготовленным злоумышленником.

В настоящее время для повышения надежности аутентификации пользователей в СЗИ применяют внешние носители ключевой информации. В технической литературе производители этих устройств и разработчики систем безопасности на их основе пользуются различной терминологией. Можно встретить подходящие по контексту термины: электронный идентификатор, электронный ключ, внешний носитель ключевой или кодовой (аутентифицирующей) последовательности. Следует понимать, что это устройства внешней энергонезависимой памяти с различным аппаратным интерфейсом, работающие в режимах чтение или

чтение/запись и предназначенные для хранения ключевой либо аутентифицирующей информации. Наиболее распространенными устройствами являются электронные ключи «TouchMemory» на базе микросхем серии DS199X фирмы DallasSemiconductors. Другое их название – «iButton» или «Далласские таблетки».

Выводы.

С точки зрения применяемых технологий аутентификации, безусловно, самой надежной является взаимная строгая двухфакторная аутентификация. В ее основе лежит технология электронной цифровой подписи (ЭЦП) с применением USB-ключей или смарт-карт в качестве надежного хранилища закрытых ключей пользователей. Под взаимностью понимается возможность проверки валидности сертификата цифровой подписи как клиента сервером, так и наоборот. Однако эта технология требует развитой инфраструктуры открытых ключей, наличия доверенной среды, а также средств проверки ЭЦП на клиентской рабочей станции. При отсутствии возможностей для выполнения этих условий, в частности, для организации удаленного доступа из недоверенной среды, были разработаны достаточно надежные схемы с применением одноразовых паролей (технология OTP – OneTimePassword). Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Одноразовый пароль действителен только для одного входа в систему. Динамический механизм задания пароля является одним из лучших способов защитить процесс аутентификации от внешних угроз. Аутентификация с применением механизма OTP является усиленной. Итак, лучшей практикой для подтверждения подлинности идентификатора является двусторонняя строгая аутентификация, основанная на технологии ЭЦП. В ситуациях, когда данную технологию использовать невозможно, необходимо применять OTP, и только при минимальном уровне рисков проникновения

злоумышленника к информационным ресурсам рекомендуется применение технологий аутентификации с помощью многоразовых паролей.

Список литературы

1. Параскевов А.В. IT диверсии в корпоративной сфере / А.В. Параскевов, И.М. Бабенков, О.Б. Шилович // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2016. – №02(116). С. 1355 – 1366. – IDA [article ID]: 1161602086. – Режим доступа: http://ej.kubagro.ru/2016/02/pdf/86.pdf, 0,75 у.п.л.

2. Основные детерминанты экономической и информационной безопасности на современном этапе развития экономики / Бабенков И.М., Параскевов А.В., Шилович О.Б. // в сборнике: Роль и место информационных технологий в современной науке - сборник статей Международной научно-практической конференции. Ответственный редактор: СукиасянАсатур Альбертович. Уфа, 2016. С. 71-74.

3. Параскевов А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / Параскевов А.В., Левченко А.В., Кухоль Ю.А. // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2015. – №06(110). – IDA [articleID]: 1101506058. – Режим доступа: http://ej.kubagro.ru/2015/06/pdf/58.pdf, 1,750 у.п.л.

4. Развитие человеческого капитала и рост национального богатства / Н.Б. Читанава, А.Н. Мейтова, О.Б. Шилович, А.В. Параскевов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №01(095). С. 1192 – 1203. – IDA [article ID]: 0951401069. – Режим доступа: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 п.л.

5. Параскевов А.В. Совершенствование управления дорожным движением (обзор) / А.В. Параскевов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2008. – №03(037). С. 207 – 217. – Шифр Информрегистра: 0420800012\0034, IDA [article ID]: 0370803014. – Режим доступа: http://ej.kubagro.ru/2008/03/pdf/14.pdf, 0,688 у.п.л.

6. Параскевов А.В. Современная робототехника в России: реалии и перспективы (обзор)/ А.В. Параскевов, А.В. Левченко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №10(104). С. 1641 – 1662. – IDA [article ID]: 1041410116. – Режим доступа: http://ej.kubagro.ru/2014/10/pdf/116.pdf, 1,375 п.л.

7. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений. – 3-е изд., стер. – М.: Издательский центр «Академия», 2008. – 336с.

8. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304с.

9. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию [Текст]. – Введ. 2000–01–01 – М.: Изд-во стандартов, 1999. – 8с.

10. ГОСТ Р 15408–02. Критерии оценки безопасности информационных технологий [Текст]. – Введ. 2004–01–01 – М.: Изд-во стандартов, 2002.

References

1. Paraskevov A.V. IT diversii v korporativnoj sfere / A.V. Paraskevov, I.M. Babenkov, O.B. Shilovich // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2016. – №02(116). S. 1355 – 1366. – IDA [article ID]: 1161602086. – Rezhim dostupa: http://ej.kubagro.ru/2016/02/pdf/86.pdf, 0,75 u.p.l.

2. Osnovnye determinanty jekonomicheskoj i informacionnoj bezopasnosti na sovremennom jetape razvitija jekonomiki / Babenkov I.M., Paraskevov A.V., Shilovich O.B. // v sbornike: Rol' i mesto informacionnyh tehnologij v sovremennoj nauke - sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii. Otvetstvennyj redaktor: SukiasjanAsatur Al'bertovich. Ufa, 2016. S. 71-74.

3. Paraskevov A.V. Sravnitel'nyj analiz pravovogo regulirovanija zashhity personal'nyh dannyh v Rossii i za rubezhom / Paraskevov A.V., Levchenko A.V., Kuhol' Ju.A. // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2015. – №06(110). – IDA [articleID]: 1101506058. – Rezhim dostupa: http://ej.kubagro.ru/2015/06/pdf/58.pdf, 1,750 u.p.l.

4. Razvitie chelovecheskogo kapitala i rost nacional'nogo bogatstva / N.B. Chitanava, A.N. Mejtova, O.B. Shilovich, A.V. Paraskevov // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №01(095). S. 1192 – 1203. – IDA [article ID]: 0951401069. – Rezhim dostupa: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 p.l.

5. Paraskevov A.V. Sovershenstvovanie upravlenija dorozhnym dvizheniem (obzor) / A.V. Paraskevov // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2008. – №03(037). S. 207 – 217. – Shifr Informregistra: 0420800012\0034, IDA [article ID]: 0370803014. – Rezhim dostupa: http://ej.kubagro.ru/2008/03/pdf/14.pdf, 0,688 u.p.l.

6. Paraskevov A.V. Sovremennaja robototehnika v Rossii: realii i perspektivy (obzor)/ A.V. Paraskevov, A.V. Levchenko // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №10(104). S. 1641 – 1662. – IDA [article ID]: 1041410116. – Rezhim dostupa: http://ej.kubagro.ru/2014/10/pdf/116.pdf, 1,375 p.l.

7. Mel'nikov V.P. Informacionnaja bezopasnost' i zashhita informacii: ucheb.posobie dlja stud. vyssh. ucheb. zavedenij. – 3-e izd., ster. – M.: Izdatel'skij centr «Akademija», 2008. – 336s.

8. Kurilo A.P., Zefirov S.L., Golovanov V.B. i dr. Audit informacionnoj bezopasnosti. – M.: Izdatel'skaja gruppa «BDC-press», 2006. – 304s.

9. GOST R 51275–99. Zashhita informacii. Ob#ekt informatizacii. Faktory, vozdejstvujushhie na informaciju [Tekst]. – Vved. 2000–01–01 – M.: Izd-vo standartov, 1999. – 8s.

10. GOST R 15408–02. Kriterii ocenki bezopasnosti informacionnyh tehnologij [Tekst]. – Vved. 2004–01–01 – M.: Izd-vo standartov, 2002.