ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.5: 65.012.8 https://doi.org/10.31713/vt4201912

Зубик Л. В., к.пед.н., доцент кафедри прикладних інформаційних систем (Київський національний університет імені Тараса Шевченка), **Зубик Я. Я., ст. викладач кафедри прикладної математики** (Національний університет водного господарства та природокористування, м. Рівне), **Іваницька А. Ю., к.т.н., асистент кафедри прикладних інформаційних систем** (Київський національний університет імені Тараса Шевченка), **Батечко О. Я., лікар-педіатр** (КНП ЦПМСД № 1 Подільського району, м. Київ)

ОРГАНІЗАЦІЙНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ СУЧАСНИХ ПРИВАТНИХ МЕДИЧНИХ УСТАНОВ

Практична діяльність окремих структур, спрямованих на захист даних і функціонуючих в установах усіх форм власності, є важливою умовою їх безпечного функціонування і розвитку. Попри стабільне підвищення вимог до систем захисту інформації, прийняття міжнародних стандартів у галузі інформаційної безпеки, збільшення витрат на розвиток систем захисту, обсяг збитків, які завдаються власникам інформаційних ресурсів, продовжує неухильно зростати. Більшість недоліків систем захисту інформації визначаються невдалими архітектурними рішеннями і стратегіями побудови системи захисту. Критична ситуація в сфері інформаційної безпеки посилюється у зв'язку з використанням глобальної мережі для проведення електронних транзакцій організацій та регулярною появою невідомих раніше типів деструктивних інформаційних впливів. Базою для комплексної системи захисту інформації є організаційні методи, за допомогою яких виконується об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації. Нові технології породжують нові види загроз, що потребує оперативного опрацювання інформації та пошуку адекватних інструментів для нівелювання їх наслідків. Найбільшу небезпеку нині складають таргетингові атаки різних типів та інсайдери. Стрімке поширення засобів масової комунікації призводить до зростання залежності суспільства від інформації. Помічено тенденцію щодо збільшення випадків атак, спрямованих на індивідуальних користувачів. Спеціалізоване медичне обладнання має низку особливос-

тей, що унеможливлюють застосування більшості стандартних технологій захисту. Активні імпланти потребують таких засобів захисту, що не впливають на роботу самого пристрою. Моніторинг та оцінка безпеки пристроїв також повинні здійснюватися незалежно від їх функціонування. Слабкі обчислювальні потужності унеможливлюють застосування в таких системах традиційних програмно-апаратних та криптографічних рішень. Статистика останніх років підтверджує той факт, що небезпека внутрішніх загроз помітно перевищує зовнішні. Питання діяльності, пов'язаної з забезпеченням надійного зберігання інформації, належать до організаційних методів захисту інформації і потребують періодичної ревізії та коригування.
Ключові слова: **методи захисту інформації, організаційні методи захисту даних.**

Вступ. Сучасний етап розвитку теорії та практики забезпечення захисту інформації характеризується суперечливою ситуацією: з одного боку, посилена увага до безпеки інформаційних об'єктів, істотне підвищення вимог щодо систем захисту інформації, прийняття міжнародних стандартів у галузі інформаційної безпеки, зростаючі витрати на забезпечення захисту, з іншого – неухильно зростаючий обсяг збитків, які завдають власникам інформаційних ресурсів, про що свідчать опубліковані дані про збитки світової економіки внаслідок комп'ютерних атак [7].

Аналіз виконаних досліджень та постановка проблеми. Проблемам підтримки інформаційної безпеки присвячені роботи таких відомих вчених як: В.Л. Бурячок [11], Б.С. Гольдштейн [3], Р.В. Грищук [10], П.М. Дев'янін [9], П.Д. Зегжда [5], А.Г. Лукацький [8], В.Ф. Шаньгин [13], А.Ю. Щербаков [14] та інші. Вагомий внесок у розвиток інформаційної безпеки внесли свого часу зарубіжні дослідники: Л.Дж. Хоффман [12]; Д.Е. Белл і Л.Дж. ЛаПадула [15]; М.А. Харрісон, У.Л. Руззо і Дж.Д. Ульман [17]; Р. Хартсон [18]; К.Дж. Лендвер [19]; Д.Д. Кларк і Д.Р. Уілсон [16] та інші. Питання безпеки глобальних мережевих технологій розглядалися в роботах А.В. Галицького [4], П.М. Дев'яніна [9], О.А. Молдовяна [6] та інших.

Наявні підходи до організації захисту інформації не забезпечують виконання сформованих до систем захисту вимог у повній мірі. Основні недоліки більшості систем захисту інформації визначаються сформованими жорсткими принципами побудови архітектури і орієнтуванням на оборонну стратегію захисту від відомих загроз. Критич-

на ситуація в сфері інформаційної безпеки посилюється у зв'язку з використанням глобальної мережі для зовнішніх і внутрішніх електронних транзакцій організації та регулярною появою невідомих раніше типів деструктивних інформаційних впливів.

Об'єкт і задачі дослідження. Для ефективного використання у будь-якій організації сучасних інформаційних технологій необхідно ефективно управляти не тільки закладом, мережею, але і системою захисту інформації. При цьому на рівні сегменту комп'ютерної інформаційної системи повинна автономно працювати окрема складова, яка реалізує управління подіями, планування модульного складу системи безпеки та перевірку її працездатності. Оскільки об'єкт управління – система захисту інформації – є досить складною організаційно-технічною системою, що постійно функціонує в умовах невизначеності, суперечливості та неповноти знань про стан інформаційного середовища, управління такою системою повинно ґрунтуватися на застосуванні системного аналізу, методів теорії прийняття рішень та необхідної інтелектуальної підтримки.

Метою дослідження є аналіз наявних організаційних методів захисту даних установ та адаптація структури системи захисту інформації до умов функціонування приватного медичного закладу.

Методи дослідження: спостереження, опитування, порівняння.

Результати досліджень. Організаційні методи захисту інформації включають як окремі планові заходи, так і стандартизовані процедури, які повинні здійснюватися посадовими особами у процесі створення й експлуатації систем для забезпечення обґрунтованого рівня захисту даних. Відповідно до діючих законів і нормативних актів у міністерствах, відомствах і на підприємствах усіх форм власності для захисту інформації створюються спеціальні служби. Зазвичай вони підпорядковуються керівництву установи, яке несе повну відповідальність за стан інформаційної безпеки. Керівники служб організують створення й функціонування систем захисту інформації.

На організаційному рівні вирішуються наступні завдання підтримки безпеки руху інформації в системі:

– організація робіт з розробки, постійної підтримки і вдосконалення системи захисту інформації;

– перевірка й оцінювання ефективності функціонування системи захисту інформації;

– обмеження й розмежування доступу до ресурсів системи;

– ліцензування діяльності щодо захисту інформації;

– сертифікація засобів захисту інформації;

– атестація об'єктів захисту;
– планування заходів;
– організація документообігу;
– навчання обслуговуючого персоналу й користувачів;
– контроль за дотриманням встановлених правил роботи в системі.

Організаційні методи є основою для комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему.

До методів і засобів організаційного захисту інформації належать організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві та ремонті приміщень, у яких буде розміщуватися система; проектуванні системи, монтажі й налагодженні її технічних і програмних складових; випробуваннях і перевірці працездатності системи.

Методи і засоби організаційного захисту вміщують:
– обмеження фізичного доступу до інформації й обладнання, реалізацію режимних заходів;
– розмежування доступу до інформаційних ресурсів і процесів (встановлення правил розмежування доступу, шифрування інформації при її зберіганні і передачі, виявлення та знищення апаратних і програмних включень);
– впровадження нових методів забезпечення надійності та відмовостійкості;
– обмеження можливості перехоплення побічних електромагнітних випромінювань і наводок;
– захист бездротових з'єднань;
– використання безпечних веб-сервісів і «хмарних» технологій;
– використання надійних систем електронно-цифрового підпису, електронних систем платежів;
– резервне копіювання найбільш важливих з точки зору втрати масивів даних;
– обмеження до мінімуму кількості осіб, які беруть участь у конфіденційних переговорах;
– візуальний огляд приміщення на предмет виявлення сторонніх пристроїв перед проведенням нарад;

– заборону перебування сторонніх осіб у приміщенні під час проведення наради;

– розроблений план дій щодо охорони виділеного приміщення під час наради, а також спостереження за обстановкою на поверсі;

– проведення будь-яких робіт, що виконуються поза часом проведення нарад (ремонт побутової техніки, ремонт приміщення, прибирання, тощо) в кімнаті для конфіденційних нарад у обов'язковій присутності працівника служби безпеки;

– ретельний огляд, закривання і опечатування кімнати після проведення наради, між нарадами кімната повинна бути закрита і опечатана відповідальною особою;

– боротьбу з сучасними витонченими методами «чорного» піару, шахрайства та дезінформації в цифровому просторі;

– профілактику зараження обладнання комп'ютерними вірусами, захист від вірусних і хакерських атак.

Базою для якісного проведення організаційних заходів є вчасне орієнтування в масиві чинних законодавчих і нормативних документів галузі інформаційної безпеки та їх практичне використання. Рішення зазначених проблем в галузі інформаційної безпеки можливе лише за умови:

– уваги до цих питань і належних цілеспрямованих дій керівників організацій і представників державної влади та громадськості;

– узгодженої діяльності національних та міжнародних органів, що займаються стандартизацією інформаційної безпеки та боротьбою з кіберзлочинністю.

Загрози інформаційної безпеки можна оцінювати, використовуючи аналітичні методи, такі як пряма експертна оцінка, статистичний аналіз, факторний аналіз. В ході прямої експертної оцінки експерти встановлюють параметри загроз, а також визначають важливість кожного з них. Статистичний аналіз заснований на накопичених даних про інциденти, до яких можна віднести частоту і джерело виникнення загрози, її успішність або невдачу. Факторний аналіз дозволяє виявити причини, які з певною ймовірністю сприяють реалізації загроз і формуванню негативних наслідків. Для аналізу потенційних загроз інформаційної безпеки доцільно застосовувати поєднання кількох розглянутих методів, що зазвичай дозволяє підвищити точність прогнозу.

Нові технології породжують нові види загроз: мініатюризація і масове використання переносних пристроїв привели до того, що сьогодні вкрай небезпечною є їх втрата. Ці проблеми особливо актуаль-

ні для організацій, адже співробітники часто використовують корпоративні пристрої поза межами периметру захисту. Втрата такого пристрою може призвести до значних фінансових втрат, а також збитків репутації компанії. Ефективним способом захисту інформації в цьому випадку є шифрування даних.

Згідно зі статистикою, на сучасному етапі найбільш поширеними є [2]:

– DDoS-атаки;
– атаки на мобільні пристрої;
– атаки через уразливості додатків і компонентів операційних систем;
– SQL-ін'єкції.

Найбільшу небезпеку нині складають таргетингові атаки різних типів та інсайдери. Стрімке поширення Інтернету, засобів масової комунікації призводить до зростання обсягів інформації, швидкостей її поширення та залежності суспільства від неї. Помічено тенденцію щодо збільшення випадків атак, спрямованих на індивідуальних користувачів. Статистика останніх років підтверджує факт, що небезпека внутрішніх загроз помітно перевищує зовнішні. Згідно з висновками експертів, витік 20% комерційної інформації в 60% випадків призводить до банкрутства компанії [1, С. 254].

Класифікуючи внутрішні загрози, можна виокремити такі важливі групи: ті, що здійснюються з корисливих або інших зловмисних міркувань, і ті, що здійснюються з необережності (некомпетентності). Навмисні витоки часто відбуваються через мережу, а випадкові – в результаті втрати обладнання. Нині одна з основних задач програмно-апаратного захисту інформації зводиться до забезпечення звичних для співробітника умов роботи та рівня інформаційного обміну із одночасним захистом даних.

Крім класичних загроз, медичне обладнання може бути пов'язане з абсолютно новим типом вразливостей в силу особливостей його використання, адже будучи кіберфізичною системою такі пристрої мають можливість фізичного впливу на здоров'я людини. Спеціалізоване медичне обладнання і такі пристрої, як бездротові активні медичні імпланти, телеманіпулятори, мають низку особливостей, що унеможливлюють застосування більшості стандартних технологій захисту, зокрема активні імпланти потребують «неінвазивних» засобів захисту, що не впливають на роботу самого пристрою. Моніторинг та оцінка безпеки пристрою також повинні здійснюватися без впливу на його поточне функціонування. Слабкі обчислюваль-

ні потужності унеможливлюють застосування в цих системах традиційних програмно-апаратних та криптографічних рішень.

Висновки. Таким чином, організаційні заходи підтримки необхідного рівня інформаційної безпеки медичної організації полягають у створенні єдиної комплексної системи захисту даних та її постійному розвитку і вдосконаленні. Окремі складові системи дозволяють ефективно протидіяти різноманітним кібернетичним загрозам насамперед шляхом їх попередження та унеможливлення. У медичних інформаційних системах, системах моніторингу, діагностичному обладнанні та системах життєзабезпечення пацієнтів необхідне застосування комплексного, проактивного і застережливого підходу для дотримання належного рівня інформаційної безпеки.

1. Гаврилов Л. П. Организация коммерческой деятельности: электронная коммерция : уч. пособ. М. : Изд-во Юрайт, 2018. 363 с. **2**. Гнусов Ю. В., Калякін С. В. Сучасні тенденції поширення кіберзагроз. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. мат. Всеукр. наук.-практ. конф. (м. Харків, 15 листопада 2017 р.). С. 28–31. **3.** Гольдштейн Б. С. Инфокоммуникационные сети и системы. СПб. : БХВ-Петербург, 2016. 208 с. **4.** Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети – анализ технологий и синтез решений. М. : ДМК Пресс, 2011. 616 с. **5.** Зегжда Д. П., Никольский А. В. Безопасность современных высокопроизводительных систем. *Безопасность облачных вычислений*. 2013. Ч. 1. 168 с. **6.** Зима В. М., Молдовян А. А. Технология практического обеспечения информационной безопасности. СПб. : Военно-космическая академия имени А. Ф. Можайского, 1997. 118 с. **7.** Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2(19). **8.** Лукацкий А. Обнаружение атак. СПб. : Издательство БХВ-Петербург, 2001. 624 с. **9.** Моделирование и верификация политик безопасности управления доступом в операционных системах : монография / П. Н. Девянин, Д. В. Ефремов, В. В. Кулямин и др. М. : Горячая линия – Телеком, 2019. 214 с. **10.** Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки : монографія / за заг. ред. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с. **11.** Бурячок В. Л., Грищук Р. В., Хорошко В. О. Політика інформаційної безпеки : підручник / під заг. ред. проф. В. О. Хорошка. К. : ПВП «Задруга», 2014. 222 с. **12.** Хоффман Л. Дж. Современные методы защиты информации. М. : Советское радио, 1980. 264 с. **13.** Шаньгин В. Ф. Информационная безопасность. М. : ДМК Пресс, 2014. 702 с. **14.** Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. М. : Издатель Молгачев С. В., 2001. 352 с. **15.** Bell David Elliott and LaPadula, Leonard J. Secure Computer Systems: Mathematical Foundations. MITRE Corporation, 1973. **16.** Clark D. D., Wilson D. R. A Comparison of Commercial and Military Computer Security Policies. May 1987, Auckland, California; IEEE Press, pp. 184–193.

17. Harrison M. A., Russo W. L., Ullman J. D. Protection in operating Systems. *Communications of the ACM*. 1976. V. I9. N 8. Pp. 461–471. **18.** Hartson R., Hsiao U. Full protection specification in the semantic model for database protection languages. *Proceedings annual Conferens ACM Houston*. New-York, 1976. Pp. 90–95. **19.** Landwehr Carl E., Bull Alan R., McDermott John P. and William S. Choi. A Taxonomy of Computer Security Flaws, with Examples. *ACM Computing Surveys*. Vol. 26, No. 3. Pp. 93–94.

REFERENCES:

1. Havrilov L. P. Orhanizatsiia kommercheskoi deiatelnosti: elektronnaia kommertsiia : uch. posob. M. : Izd-vo Yurait, 2018. 363 s. **2.** Hnusov Yu. V., Kaliakin S. V. Suchasni tendentsii poshyrennia kiberzahroz. *Aktualni pytannia protydii kiberzlochynnosti ta torhivli liudmy* : zb. mat. Vseukr. nauk.-prakt. konf. (m. Kharkiv, 15 lystopada 2017 r.). S. 28–31. **3.** Holdshtein B. S. Infokommunikatsionnye seti i sistemy. SPb. : BKhV-Peterburh, 2016. 208 s. **4.** Halitskii A. V., Riabko S. D., Shanhin V. F. Zashchita informatsii v seti – analiz tekhnolohii i sintez reshenii. M. : DMK Press, 2011. 616 s. **5.** Zehzhda D. P., Nikolskii A. V. Bezopasnost sovremennykh vysokoproizvoditelnykh sistem. *Bezopasnost oblachnykh vychyslenii*. 2013. Ch. 1. 168 s. **6.** Zima V. M., Moldovian A. A. Tekhnolohiia prakticheskoho obespecheniia informatsionnoi bezopasnosti. SPb. : Voenno-kosmicheskaia akademiia imeni A. F. Mozhaiskoho, 1997. 118 c. **7.** Kravtsova M. O. Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini. *Visnyk kryminolohichnoi asotsiatsii Ukrainy*. 2018. № 2(19). **8.** Lukatskii A. Obnaruzhenie atak. SPb. : Izdatelstvo BKhV-Peterburh, 2001. 624 s. **9.** Modelirovanie i verifikatsiia politik bezopasnosti upravleniia dostupom v operatsionnykh sistemakh : monohrafiia / P. N. Devianyn, D. V. Efremov, V. V. Kuliamyn y dr. M. : Horiachaia liniia – Telekom, 2019. 214 s. **10.** Hryshchuk R. V., Danyk Yu. H. Osnovy kibernetychnoi bezpeky : monohrafiia / za zah. red. Yu. H. Danyka. Zhytomyr : ZhNAEU, 2016. 636 s. **11.** Buriachok V. L., Hryshchuk R. V., Khoroshko V. O. Polityka informatsiinoi bezpeky : pidruchnyk / pid zah. red. prof. V. O. Khoroshka. K. : PVP «Zadruha», 2014. 222 s. **12.** Khoffman L. Dzh. Sovremennye metody zashchity informatsii. M. : Sovetskoe radio, 1980. 264 s. **13.** Shanhin V. F. Informatsionnaia bezopasnost. M. : DMK Press, 2014. 702 s. **14.** Shcherbakov A. Yu. Vvedenie v teoriiu i praktiku kompiuternoi bezopasnosti. M. : Izdatel Molhachev S. V., 2001. 352 s. **15.** Bell David Elliott and LaPadula, Leonard J. Secure Computer Systems: Mathematical Foundations. MITRE Corporation, 1973. **16.** Clark D. D., Wilson D. R. A Comparison of Commercial and Military Computer Security Policies. May 1987, Auckland, California; IEEE Press. Pp. 184–193. **17.** Harrison M. A., Russo W. L., Ullman J. D. Protection in operating Systems. *Communications of the ACM*. 1976. V. I9. N 8. Pp. 461–471. **18.** Hartson R., Hsiao U. Full protection specification in the semantic model for database protection languages.

Proceedings annual Conferens ACM Houston. New-York, 1976. Pp. 90–95. **19.** Landwehr Carl E., Bull Alan R., McDermott John P. and William S. Choi. A Taxonomy of Computer Security Flaws, with Examples. *ACM Computing Surveys*. Vol. 26, No. 3. Pp. 93–94.

Zubyk L. V., Candidate of Pedagogical Sciences (Ph.D.), Associate Professor, Department of Apply Information Systems (Taras Shevchenko National University of Kyiv, Kyiv), **Zubyk Y. Y., Senior Lecturer, Department of Apply Mathematic** (National University of Water and Environmental Engineering, Rivne), **Ivanytska A. Y., Candidate of Engineering (Ph.D.), Associate Professor, Department of Apply Information Systems** (Taras Shevchenko National University of Kyiv, Kyiv), **Batechko O. Y., Paediatrician** (MNPE CPHC # 1 of Podilskyi District of Kyiv)

ORGANIZATIONAL METHODS OF INFORMATION PROTECTION OF MODERN PRIVATE MEDICAL INSTITUTIONS

The practical activity of individual data protection structures and institutions that operating in all forms of ownership is an important condition for their secure functioning and development. Despite the steady increase in the requirements for information security systems, the adoption of international standards in the field of information security, the increasing costs for the development of security systems, the amount of damage inflicted on the owners of information resources continues to grow steadily. Most deficiencies in information security systems are determined by poor architectural solutions and strategies for building a security system. The critical situation in the field of information security is exacerbated by the use of the global network for electronic transactions of organizations and the regular appearance of previously unknown types of destructive information impacts. The basis for a comprehensive information security system is the organizational methods by which legal, technical, software and cryptographic information security systems are integrated. New technologies create new types of threats that require prompt processing of information and finding adequate tools to counteract their effects. The biggest danger now is targeting attacks of various types and insiders. The rapid proliferation of mass media has led to an increase in society's dependence on information. There has been a tendency for an increase in individual-targeted attacks. Specialized

medical equipment has a number of features that make it impossible to use most standard protection technologies. Active implants require protection that does not affect the operation of the device itself. The monitoring and evaluation of the safety of devices must also be carried out regardless of their operation. Weak computing power makes it impossible to use traditional hardware and cryptographic solutions in such systems. Recent years' statistics confirm the fact that the danger of internal threats far outweighs the external ones. Issues related to the secure storage of information relate to organizational information security practices and require periodic review and adjustment.
***Keywords*: methods of information protection, organizational methods of data protection.**

Зубик Л. В., к.п.н., доцент кафедры прикладных информационных систем (Киевский национальный университет имени Тараса Шевченко, Киев)**, Зубик Я. Я., ст. преподаватель кафедры прикладной математики** (Национальный университет водного хозяйства и природопользования, г. Ровно)**, Иваницкая А. Ю., к.т.н., ассистент кафедры прикладных информационных систем** (Киевский национальный университет имени Тараса Шевченко, Киев)**, Батечко О. Я., врач-педиатр** (КНП ЦПМСП № 1 Подольского района, г. Киев)

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ СОВРЕМЕННЫХ ЧАСТНЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

Практическая деятельность отдельных структур, направленных на защиту данных и функционирующих в учреждениях всех форм собственности, является важным условием их безопасного функционирования и развития. Несмотря на стабильное повышение требований к системам защиты информации, принятия международных стандартов в области информационной безопасности, увеличение расходов на развитие систем защиты, объем убытков, которые наносятся владельцам информационных ресурсов, продолжает неуклонно расти. Большинство недостатков систем защиты информации определяются неудачными архитектурными решениями и стратегиями построения системы защиты. Критическая ситуация в сфере информационной безопасности усиливается в связи с

использованием глобальной сети для проведения электронных транзакций организаций и регулярной появлением неизвестных ранее типов деструктивных информационных воздействий. Базой для комплексной системы защиты информации являются организационные методы, с помощью которых выполняется объединение на правовой основе технических, программных и криптографических средств защиты информации. Новые технологии порождают новые виды угроз, что требует оперативной обработки информации и поиска адекватных инструментов для нивелирования их последствий. Наибольшую опасность в настоящее время составляют таргетинговые атаки различных типов и инсайдеры. Стремительное распространение средств массовой коммуникации приводит к росту зависимости общества от информации. Замечена тенденция по увеличению случаев атак, направленных на индивидуальных пользователей. Специализированное медицинское оборудование имеет ряд особенностей, которые делают невозможным применение большинства стандартных технологий защиты. Активные импланты требуют таких средств защиты, которые не влияют на работу самого устройства. Мониторинг и оценка безопасности устройств также должны осуществляться независимо от их функционирования. Слабые вычислительные мощности делают невозможным применение в таких системах традиционных программно-аппаратных и криптографических решений. Статистика последних лет подтверждает тот факт, что опасность внутренних угроз заметно превышает внешние. Вопросы деятельности, связанной с обеспечением надежного хранения информации, относятся к организационным методам защиты информации и нуждаются в периодической ревизии и корректировке.
***Ключевые слова*: методы защиты информации, организационные методы защиты данных.**