6. *А. Р. Марковский, Бесанар Карим, В.А. Баканов, В.А. Хорошко.* Критерии оценки эффективности сложных систем. Моделювання та іформаційні технології. Зб.наук, праць ІПМЕ НАНУ. - 1999.-№2. - С. 156- 159.

7. *Саати Т., Керис К.* Аналитическое планирование. Организация систем: Пер. с англ. -М.: Радио и связь, 1991.-458 с.

Работа посвящена выбору показателей эффективности мер защиты информации, которые определяются такими факторами, как назначение методик; технология оценки эффективности и выбора мер ЗИ; целевое назначение мер ЗИ, которое заключается в предотвращении ущерба субъектам информационных отношений на предприятии от угроз нарушения безопасности информации.

Робота присвячена вибору показників ефективності заходів захисту інформації, які визначаються такими чинниками, як призначення методик; технологія оцінки ефективності і вибору заходів ЗІ; цільове призначення заходів ЗІ, яке полягає в запобіганні збитку суб'єктам інформаційних відносин на підприємстві від загроз порушення безпеки інформації.

Work is devoted the choice of indexes of efficiency of measures of ZI, which are determined such factors, as setting of methods; technology of estimation of efficiency and choice of measures of ZI; having a special purpose setting of measures of ZI, which consists in prevention of harm the subjects of informative relations on an enterprise from the threats of security of information breach

Рецензент: д.т.н., проф. Корнійчук М.Т.

Надійшла 06.01.2011

УДК 004.056 **Єжова Л.Ф. (ДУІКТ)**

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ : ТЕХНОЛОГІЇ І ПЕРСОНАЛ

ВСТУП

Діяльність будь-якої організації у наш час пов'язана з отриманням і передачею інформації. Більш того, кожному реальному об'єкту чи суб'єкту організації відповідає певний інформаційний актив, який потребує захисту. Інформація стала стратегічно важливим товаром. Втрата інформаційних ресурсів або заволодіння секретною інформацією конкурентами, може завдати підприємству значних збитків і навіть може привести до банкрутства.

Інформаційна безпека (ІБ) має здатність до деградації, коли не відбуваються її суттєві порушення і створюється ілюзія цілковитої безпеки, тоді не зберігаються у таємниці паролі, не відслідковуються відвідувачі організації тощо. Тому в сьогоднішній ситуації підприємства повинні мати стратегію ІБ, яка ґрунтується на комплексному підході, здійснювати контроль всіх параметрів ІБ, мати систему заходів з оцінки відповідності інформаційних систем підприємства певним стандартам та вимогам, мати процедури оцінки ризиків, пов'язаних з використанням інформаційних технологій та участю персоналу в них.

МЕТОЮ даної роботи є дослідження ролі персоналу в проведенні аудиту інформаційної безпеки технологічних процесів на об'єкті.

Серед процесів контроля та перевірки ІБ особливу роль відіграє аудит ІБ, основним призначенням якого є формування незалежної оцінки ІБ організації, незалежної від діяльності, яка перевіряється.

Зауважимо, що в такому випадку висновок про те, наскільки успішно функціонує об'єкт і наскільки він відповідає всім вимогам, робиться на основі вивчення якості виконання персоналом цього об'єкта відповідних функцій, зафіксованих у технологічних регламентах, створених по встановлених стандартах.

Через специфіку області інформаційної безпеки фундаментальну роль і місце має думка (суб'єктивне відчуття) людини. Небезпека і безпека, як її протилежність, є умогляд-

ймовірностні категорії, причому ймовірності тут також умовні, оскільки, як правило, відсутні статистики по багатьох аспектах, унікальних у кожному окремому випадку. Аудит ІБ, поряд з іншими методами довіри, може бути значним інструментом забезпечення впевненості в інформаційній безпеці.

За своєю суттю цей метод є прогностичним, отже висновки по результатах аудиту мають принципово ймовірностно-прогностичний характер. Тому документи, складені за результатами аудиту, містять не тільки оцінні звіти, а й конкретні та жорсткі рекомендації щодо приведення внутрішніх процесів і регламентів до відповідності загальноприйнятим стандартам або практикам.

Останнім часом маємо позитивний досвід застосування методології аудиту для оцінки складних систем, у першу чергу таких, функціонування яких нерозривно пов'язана з діяльністю колективів людей, відношення між якими є визначальним фактором успішної діяльності цих систем. Складність полягає в тому, що оцінити роботу персоналу можна тільки методами аудиту, а технічних систем — методом випробувань або спостережень з накопиченням інформації для подальшої оцінки ризиків.

Аудит – ефективний засіб підтримки режиму інформаційної безпеки. Аудит інформаційної безпеки – це системний методичний, незалежний і документований процес, відповідний до стандартів та процедур аудиту, отримання і об'єктивної оцінки даних щодо поточного стану інформаційної безпеки системи для з'ясування їх відповідності певним критеріям. Це також перевірка інформаційних систем, систем безпеки, систем зв'язку із зовнішнім середовищем корпоративної мережі, на предмет їх відповідності бізнес-процесам компанії, відкритим міжнародним і державним стандартам аудиту інформаційної безпеки, закритим (корпоративним) стандартам аудиту, внутрішнім нормативним документам з наступною оцінкою ризиків збою в їх функціонуванні.

Отже, аудит – це перевірка на відповідність політикам / процедурам по ІБ; вимогам контрактів/клієнтів; законодавчим/обов'язковим вимогам; документації по ІБ; стандартам організації; вимогам ISO 27001: 2005.

Для будь-якої організації (підприємства) об'єктивно існують такі види аудиту:

– співробітники організації перевіряють свою систему інформаційної безпеки (внутрішній аудит);

– співробіники організації перевіряють постачальника або організацію перевіряє замовник чи користувач (зовнішній аудит);

– організацію перевіряє незалежний орган із сертифікації (зовнішній аудит).

Процес аудиту інформаційної безпеки починається з розробки плану і програми, яка базується на визначенні *задач, області діяльності, критеріїв*.

Задачі аудиту ІБ:

- Визначити степінь відповідності звітної документації з ІБ або її складових критеріям аудиту;
- Оцінити здатність документації з ІБ забезпечити відповідність діючому законодавству та контрактним зобов'язанням;
- Оцінити, наскільки ефективно документація з ІБ задовольняє конкретним задачам;
- Виявити області потенційного покращення документації з ІБ.

Область охоплення аудиту визначає глибину та границі аудиту, а саме:

- Підрозділи організації;
- Їх розташування;
- Види діяльності організації;
- Її бізнес-процеси;
- Інформаційні активи;
- Ризики;
- Період проведення аудиту.

Критерії аудиту повинні містити:

- Політику ІБ;

- Процедури системи менеджмента ІБ;
- Стандарти (ISO 27001:2005 та інш.);
- Вимоги законодавства;
- Вимоги менеджменту ІБ;
- Контрактні обов'язки;
- Норми та кращі практики сфери ІБ;
- тощо.

Звичайно, для зовнішнього та внутрішнього аудиту задачі, області охоплення, критерії будуть відрізнятись.

У зовнішньому аудиті можна виділити такі головні комплекси завдань:

- оцінювання компетентності і професіоналізму адміністрації за аналізований період;
- оцінювання достовірності системи обліку подій, що відбувалися у системі ІБ на підприємстві;
- оцінювання правильності дій персоналу щодо фіксації стану ІБ інформаційної системи;
- консультування щодо поліпшення ІБ підприємства і прогнозування подальших подій.

Звичайно ж кожний такий комплекс складається із завдань, які можна формалізувати для реалізації в комп'ютерній системі. Інформаційна база даних зовнішнього аудиту складається з локальних файлів, тому що вона не належить підприємству, а приноситься ззовні. Вони не можуть залежати від конкретної інформаційної системи та способу організації даних на підприємстві, оскільки програми обробки даних зовнішнього аудиту можуть бути з ними не сумісні. Систему зовнішнього аудиту представлено на рис.1.

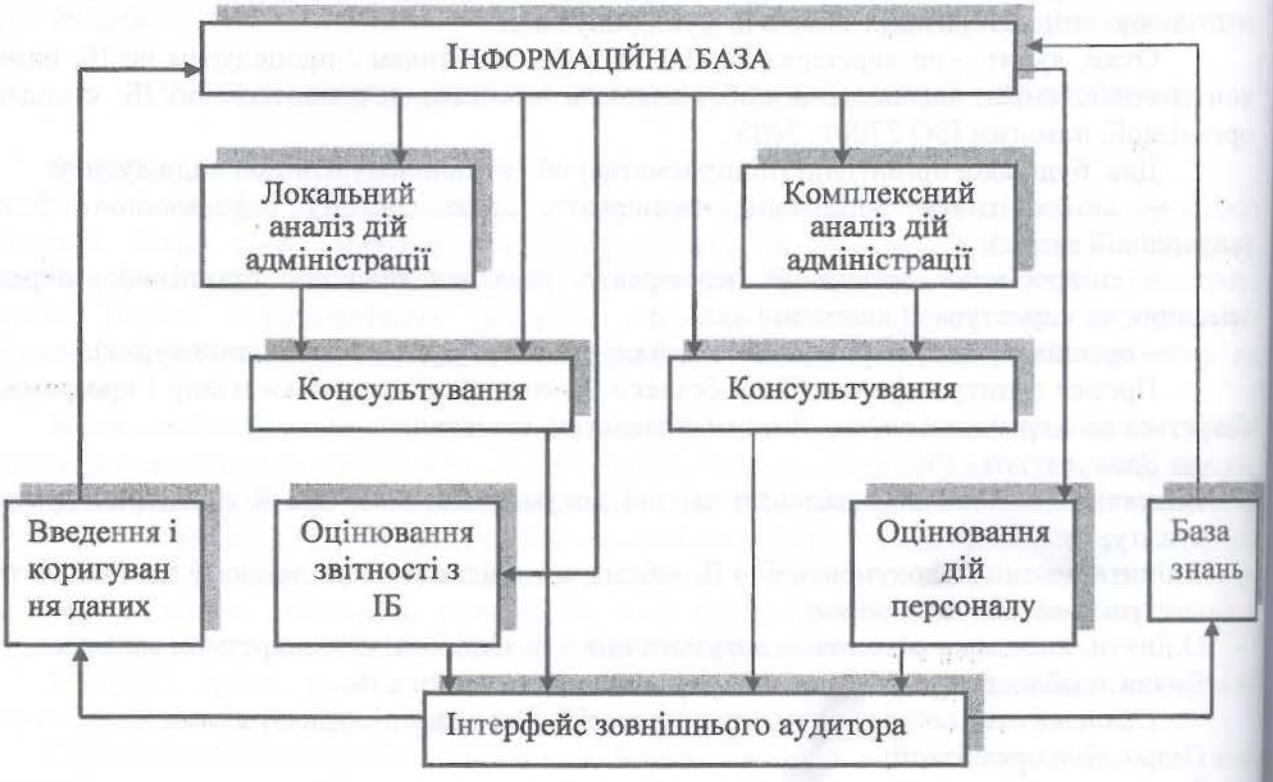

Рис.1 Система зовнішнього аудиту

Система зовнішнього аудиту спрямована, в першу чергу, на захист інформаційної системи в цілому. Щодо аудиту організації захисту інформації на адміністративному рівні, то тут спрацьовує людський фактор і сподіватись на об'єктивну оцінку результатів внутрішнього аудиту навряд чи доцільно.

Крім того, в обов'язки зовнішніх аудиторів не входить інвентаризація, доскональна перевірка правильності переоцінки основних засобів і ряд інших питань. Розв'язати вказані проблеми допомагає служба внутрішнього аудиту.

Внутрішній аудит дає інформацію вищій ланці управління про стан дотримання режиму ІБ, сприяє створенню високоефективної системи внутрішнього контролю, яка перешкоджає виникненню порушень. Внутрішній аудит дає об'єктивну оцінку поточного стану інформаційної безпеки системи, а саме програмно-технічних засобів, щоб з'ясувати їх відповідність певним критеріям безпеки. Систему внутрішнього аудиту представлено на рис.2.

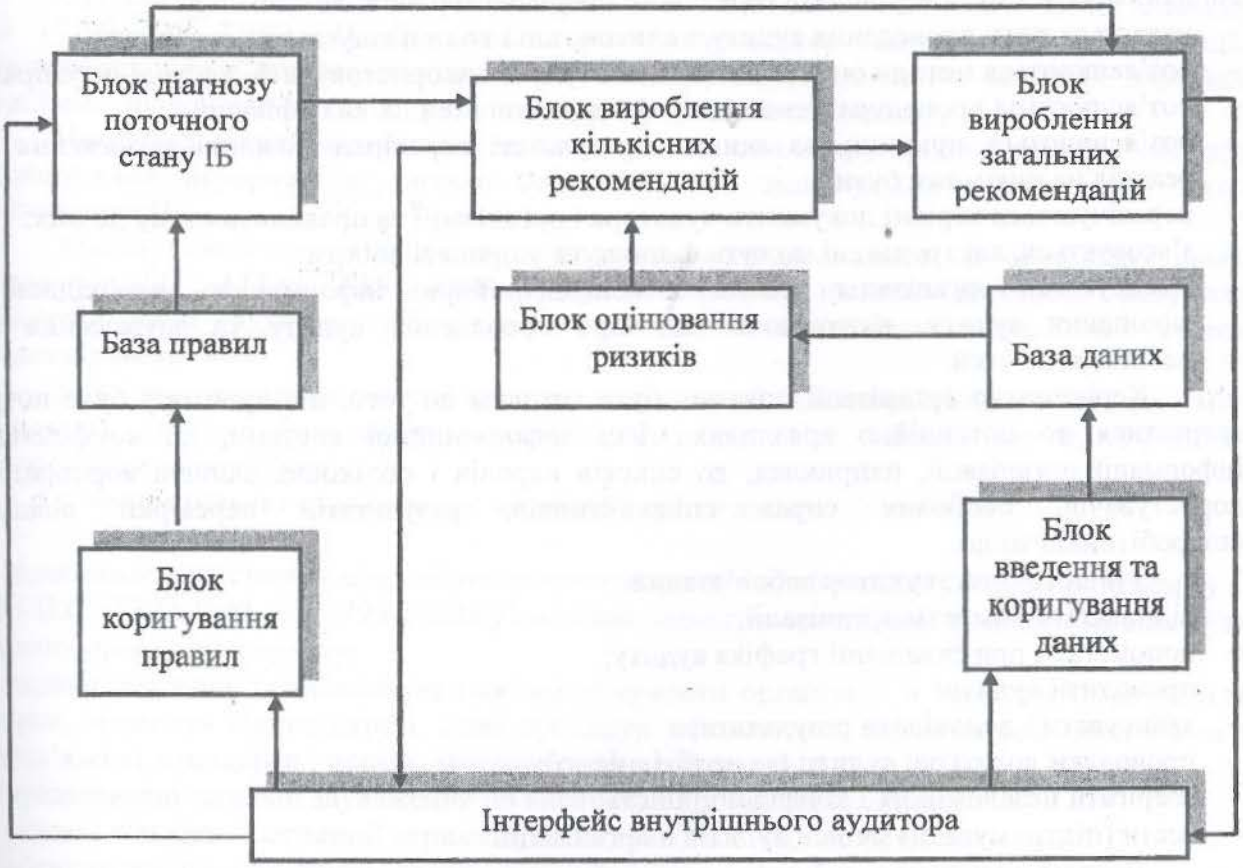

Рис.2 Експертна система внутрішнього аудиту

Основними функціями внутрішнього аудиту є контрольно-ревізійна та консультативно-прогнозна. Відповідно до цього у внутрішньому аудиті можна виділити такі головні комплекси завдань:

- оцінювання достовірності системи обліку подій, що відбувалися у системі ІБ на підприємстві;
- оцінювання правильності дій персоналу щодо фіксації стану ІБ інформаційної системи;
- перевірка дотримання національних та корпоративних стандартів, внутрішніх інструкцій щодо ІБ;
- інвентаризація основних засобів забезпечення ІБ;
- локальне і комплексне діагностування системи ІБ;
- консультування щодо поліпшення ІБ підприємства і прогнозування подальших подій.

Отже система внутрішнього аудиту відрізняється від системи зовнішнього аудиту функціями, джерелами інформації, потенційними користувачами.

Внутрішній аудит необхідний для організації, щоб визначити, наскільки задачі, засоби контролю, процедури та документація системи управління ІБ відповідають вимогам

стандартів і законодавству, наскільки засоби ІБ ефективно впроваджені, підтримуються і функціонують в очікуваному режимі.

Користь від внутрішнього аудиту полягає втому, що відбувається:

- перевірка відповідності політиці та процедурам ІБ;
- надання неупередженої інформації керівництву організації для аналізу;
- збільшення обізнаності співробітників у сфері ІБ;
- визначення можливостей для покращення системи управління ІБ та прийняття відповідних рішень у сфері ІБ.

Роботи по аудиту інформаційної безпеки завжди розпочинаються з офіційних зборів співробітників з ІБ та керівників середнього і верхнього рівнів, де:

- надається план проведення аудиту з описом, що і коли планується перевіряти;
- роз'яснюються методи оцінки ризиків, які будуть використовуватися у ході перевірки;
- роз'яснюється процедура визначення невідповідностей, їх кваліфікація і
- роз'яснюються причини, за якими в результаті перевірки можливі зауваження і яка реакція на них може бути;
- перелічуються керівні документи аудитора і організації та правила доступу до них;
- з'ясовується, які труднощі можуть виникнути у процесі роботи;
- з'ясовується організація роботи з конфіденційною інформацією, необхідною для виконання аудиту, включаючи звіт про проведення аудиту та зауваження щодо невідповідностей.

Керівництво організації повинно бути готовим до того, що аудитору буде потрібно звертатися до потенційно вразливих місць інформаційної системи, до конфіденційної інформації організації, наприклад, до списків паролів і облікових записів корпоративних користувачів, особових справ співробітників, результатів перевірки лояльності співробітників тощо.

З іншого боку, аудитор зобов'язаний:

- відповідати вимогам організації;
- допомагати при складенні графіка аудиту;
- проводити аудити;
- записувати і доповідати результати;
- проводити додаткові аудити (за необхідністю);
- зберігати незалежність і конфіденційність;
- вести (підтримувати) записи аудитів в організації.

Доброю практикою аудитора є правила:

- задавайте питання потрібній людині – людині, яка наділена повноваженнями в області, яку ви перевіряєте;
- формулюйте питання чітко, зрозуміло, простою мовою. уникайте жаргонів і специфічних професійних скорочень;
- давйте час інтерв'юйованому відповісти на ваші питання;
- не ставайте на чийсь бік, залишайтесь неупередженим, не робіть скороспішних висновків, завжди шукайте докази;
- будьте ввічливими у будь-якій ситуації, не звертаючи уваги на провокації, з якими ви можете зустрітись.

Поганою практикою аудитора є:

- задавати надто багато питань одночасно;
- казати, що "розумієш", коли не розумієш;
- вступати в суперечки;
- критикувати будь-кого;
- приставати на чийсь бік.

Щоб уникнути зайвих ускладнень, необхідно: заздалегідь сповістити про аудит, пояснити всім співучасникам значимість аудиту, вміти поставити себе на місце

інтерв'юйованого, уважно слухати і демонструвати розуміння, повідомляти людей про виявлені в процесі аудиту недоліки та невідповідності.

За результатами аудиту складається список зауважень, виявлених невідповідностей вимогам стандартів і рекомендацій по їх виправленню.

Невідповідність – це ситуація, де існує ймовірність, що може відбутися інцидент ІБ або очевидна відсутність чи недостатня відповідність вимогам політики / процедури ІБ.

Аудитори повинні гарантувати виконання всіх вимог процедури аудиту. Щоб визначити, наскільки серйозні виявлені невідповідності, треба скористатися стандартом, де розглянуті такі категорії невідповідностей:

Суттєва невідповідність – не виконується одна чи декілька базових вимог стандарту ISO 17799 (BS 7799) [4] або встановлено використання неадекватних заходів щодо забезпечення конфіденційності, цілісності чи доступності критично важливої інформації організації, що приводять до неприпустимого інформаційного ризику;

Несуттєва невідповідність – не виконуються деякі другорядні вимоги, чим дещо підвищуються інформаційні ризики організації або зменшується ефективність заходів забезпечення ІБ.

Кожна виявлена невідповідність повинна мати посилання на відповідну вимогу стандарту ISO 17799 (BS 7799). При виявленні значної кількості несуттєвих невідповідностей аудитор зобов'язаний дослідити можливість виникнення суттєвої невідповідності.

Звіт про невідповідність містить: унікальний ідентифікаційний номер; місце (підрозділ), де була виявлена невідповідність; дату; зміст вимоги; що є об'єктивним свідоцтвом невідповідності.

Головним результатом аудиту є офіційний звіт, в якому:

- відображається степінь відповідності комп'ютерної інформаційної системи стандарту BS ISO / IEC 17799:2000 (BS 7799-1:2000) і власним вимогам організації в області ІБ відповідно до плану проведення аудиту;
- надано докладне посилання на основні документи організації в тому числі на політику безпеки, відомість відповідності, опис процедур забезпечення ІБ, додаткові обов'язкові та необов'язкові стандарти і норми, застосовувані в цій організації;
- представлені загальні зауваження по висновках проведення аудиту;
- вказані кількість і категорії отриманих невідповідностей і зауважень;
- обгрунтована необхідність додаткових дій з аудиту (якщо це необхідно) і складений їх загальний план;
- приведений список співробітників, що брали участь у тестуванні.

Зазначені стандарти, узагальнивши найпередовіші досягнення в організації інформаційної безпеки підприємства чи організації, повинні стати нормою взаємовідносин між діловими партнерами.

За результатами перевірки аудитор може сформулювати у звітних документах зауваження, якщо він припускає можливість удосконалення підсистеми ІБ комп'ютерної інформаційної системи [3].

Наступні дії організації можуть бути, наприклад, такими:

- організація готує план коригуючих дій;
- організація надає план аудитору;
- аудитор оцінюєї план;
- організація виконує план;
- організація оцінює ефективність;
- організація переглядає план за необхідністю;
- організація документує зміни;
- аудитор перевіряє виконання та ефективність виконаних заходів;
- ведуться записи по всіх здійснених заходах (і аудитором, і організацією).

Але реакція організації на зауваження аудитора може бути іншою, оскільки організації самі добровільно визначають свої дії щодо усунення зауважень.

Наступні дії аудитора можуть бути, наприклад, такими:

- додаткова перевірка в тому підрозділі, де була знайдена невідповідність;
- аналіз документації;
- перевірка при наступному аудиті;
- домовленість про наступний аудит.

На закінчення необхідно відзначити, що аудит інформаційної безпеки повинен містити у собі і проведення безпосередньої перевірки безпеки (pen testing) тобто цілеспрямовану перевірку наявності уразливих місць у критичних ресурсах системи. Така перевірка виконується тестуванням як на проникнення у систему ззовні, так і всередині системи. Бажано, щоб системні адміністратори і персонал організації по можливості не знали про тестування інформаційної системи під час його проведення.

ВИСНОВКИ

Персонал – головний актив будь-якої організації. Практично стан її інформаційної безпеки залежить саме від персоналу. Аудит є тим інструментом, який допоможе встановити не тільки степінь залежності стану інформаційної безпеки від персоналу, але й визначити ті адміністративні заходи, які сприятимуть підвищенню її рівня.

Література

1. Information security management. Part 2. Specification for information security management systems. British Standard BS 7799. Part 2. 1998.
2. Code of practice for Information Security Management. British Standard BS 7799, 1995.
3. BSI Management Systems Training – London, 2004.
4. Information security management. Part 1.British Standard BS 7799-1:2000

Розглянуті особливості розробки технологій проведення аудиту інформаційної безпеки на основі Британського стандарту BS 7799 з урахуванням людського фактору.

Рассмотрены особенности разработки технологий проведения аудита информационной безопасности на основе Британского стандарта BS 7799 с учетом человеческого фактора.

The features of the development of technology auditing information security based on British Standard BS 7799, taking into account the human factor/

Рецензент: д.т.н., проф. Рибальський О.В.
Надійшла 24.01.2011

УДК 004.056.55:34

Слепцов В. И. Лизунов С.И.

СООБЩЕНИЯ КАК ФОРМА ИНФОРМАЦИИ, СРЕДСТВО ПОЗНАНИЯ И ПРЕДМЕТ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Вступление

Одним из важнейших направлений информационной деятельности является получение информации индивидом для удовлетворения своих потребностей и, прежде всего, потребности в познании. Как известно, познание представляет собой процесс приобретения и развития знания, его углубления и расширения. Предопределяют возможность и успешность познания полнота и достоверность информации об окружающем мире, доступной для потребителя, и его интеллектуальный потенциал. Отсюда важность определения понятия информации, как средства познания, выделения и классификация составляющих процесса познания, выяснения возможности (необходимости) правового регулирования этого процесса.