УДК 659.4:004.9

Чубукова О.Ю.
доктор економічних наук, професор,
завідувач кафедри економічної кібернетики та маркетингу
Київського національного університету технологій та дизайну

Пономаренко І.В.
кандидат економічних наук, доцент,
доцент кафедри економічної кібернетики та маркетингу
Київського національного університету технологій та дизайну

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

АНОТАЦІЯ

У статті представлено поточну ситуацію щодо здійснення кібератак на компанії світу. Наведено основну статистичну інформацію про втрати від незаконних дій з інформацією компаній. Визначено орієнтацію злочинних угруповань на незаконні маніпуляції з даними компаній для отримання економічної вигоди. Доведено важливість забезпечення ефективної системи інформаційної безпеки компаній. Представлено основні етапи забезпечення інформаційної безпеки, які повинні міститися у відповідній стратегії компанії.

Ключові слова: інформаційна безпека, бази даних, ефективність, кібербезпека, Інтернет.

АННОТАЦИЯ

В статье представлена текущая ситуация по осуществлению кибератак на компании мира. Приведена основная статистическая информация о потерях от незаконных действий с информацией компаний. Определена ориентация преступных группировок на незаконные манипуляции с данными компаний для получения экономической выгоды. Доказана важность обеспечения эффективной системы информационной безопасности компаний. Представлены основные этапы обеспечения информационной безопасности, которые должны содержаться в соответствующей стратегии компании.

Ключевые слова: информационная безопасность, базы данных, эффективность, кибербезопасность, Интернет.

ANNOTATION

The article presents the current situation regarding the implementation of cyber attacks on the world's companies. The main statistical information about losses from illegal actions with company information is given. It is determined the targeting of criminal gangs against illegal manipulations with these companies to obtain economic benefits. The importance of providing an effective information security system for companies is proved. The main stages of ensuring information security are presented, which should be contained in the company's respective strategy.

Key words: information security, databases, efficiency, cyber security, Internet.

Постановка проблеми у загальному вигляді та її зв'язок із важливиминауковими чи практичними завданнями. Особливості функціонування сучасних підприємств, установ та організацій передбачають переведення системи документообліку в електронний вигляд. Створення спеціалізованих баз даних, які містять комплексні відомості про діяльність зазначених структур та їх окремих підрозділів, інформацію про певних працівників або інших юридичних або фізичних осіб, що пов'язані із цими закладами, дає можливість швидко отримувати необхідні дані. Компанії приділяють увагу забезпеченню захисту більшості інформаційних ресурсів, оскільки вони містять цінні персональні відомості про окремі категорії працівників, а також діяльність зазначених організацій, що можуть бути вкрадені та використані третіми особами для отримання певного зиску, а також призведуть до матеріальної та моральної шкоди. Окреслені проблеми необхідно вирішувати на постійній основі, оскільки науково-технічний прогрес призводить до еволюції шкідливого програмного забезпечення та спеціалізованих шпигунських пристроїв. Для мінізації ризиків утрати цінної інформації існує потреба в комплексному дослідженні особливостей захисту даних та реалізації передового досвіду у сфері протидії кіберзлочинам у практичній діяльності компаній [1; 2].

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язанняданої проблеми і на які спираються автори. Дослідженню питань інформаційної безпеки присвячено праці таких учених, як В. Гібсон, С. Гнатюк, О. Довгань, Д. Дубов, М. Лібіцкі, Дж. Льюіс, С. Мельник, С. Старр, В. Харченко та ін. Проте існує необхідність у дослідженні ситуації з безпекою даних у різноманітних компаніях та розроблення комплексу заходів щодо забезпечення ефективної системи протидії кібератакам.

Виділення невирішених раніше частин загальної проблеми, котримприсвячується означена стаття. Комплексний аналіз інформаційної безпеки є складним та багатоаспектним процесом, який передбачає витрати значних фінансових ресурсів та часу, оскільки цифрове середовище розвивається під впливом великої кількості чинників, що постійно трансформуються. Активізація боротьби між компаніями – власниками інформаційних ресурсів та зловмисниками, що прагнуть збагатитися завдяки певним маніпуляціям із даними, призводить до залучення фінансових, матеріальних, людських та часових ресурсів з обох боків. Дослідження цієї наукової проблеми дає можливість оптимізувати систему інформаційної безпеки компаній.

Формулювання цілей статті **(постановка завдання).** Метою статті є дослідження особливостей забезпечення інформаційної безпеки в сучасних умовах.

Виклад основного матеріалу дослідження з повним обґрунтуваннямотриманих наукових результатів. У сучасних умовах спостерігається зростання інформаційного середовища внаслідок збільшення кількості учасників, що

інтегруються до цифрового середовища та створюють додаткові обсяги даних. Інформатизація суспільства призвела до трансформації даних у цінний ресурс, який має певну вартість та розглядається зловмисниками як засіб збагачення внаслідок її викрадення, пошкодження або знищення.

Для здійснення незаконних дій з інформацією зловмисники використовують спеціалізоване програмне забезпечення. У 2017 р. об'єктами атак стали здебільшого інфраструктура і веб-ресурси компаній. Нині у структурі шкідливого програмного забезпечення перше місце посіли трояни-шифрувальники. Проблему представляють не стільки вимагачі, скільки віруси, які безповоротно шифрують дані, завдаючи тим самим величезної шкоди інфраструктурі компаній.

На рис. 1 представлено середній економічний збиток від кібератак на підприємства в усьому світі станом на квітень 2018 р.

Отримані дані свідчать, що найбільша питома вага компаній (30%) зазнала матеріальних збитків унаслідок кібератак – понад 100 тис. дол. США на одну юридичну особу. Поряд із цим 38% компаній утратили понад 1 млн. дол. США у розрахунку на одну юридичну особу. Представлені результати свідчать про існування потреби в інтенсифікації розроблення інноваційних засобів захисту від кібератак. Зазначені заходи необхідно реалізовувати на постійній основі, оскільки перспективність збагачення за рахунок незаконного заволодіння даними або інших злочинних маніпуляцій з інформацією спонукає злочинців удосконалювати відповідне шкідливе програмне забезпечення.

На рис. 2 представлено розподіл компаній за найбільшою кількістю скомпрометованих записів персональних даних станом на листопад 2018 р.

Активне використання населенням мережі Інтернет, у тому числі й соціальних мереж, призводить до посилення ризиків утручання у приватне життя користувачів. Поряд із моральною шкодою також існує високий ризик утрати грошових коштів унаслідок дій злочинців. Зазначений ризик посилюється завдяки віртуалізації фінансової системи та зростанню кількості користувачів, що оплачують послуги в Інтернеті за допомогою системи онлайн-банкінгу.

Необхідно відзначити, що особливості розміщення, зберігання, використання та захисту інформації в різних компаніях впливають певним чином на специфіку незаконних маніпуляцій із даним. На рис. 3 представлено результати опитування керівників міжнародних компаній стосовно ризику кібератак у розподілі за основними напрямами.

Згідно з представленими результатами, найбільша кількість ризиків кібератак пов'язана з бажанням злочинців (злочинні угруповання та хакерські групи) отримати економічну вигоду внаслідок незаконних маніпуляцій із даними. Важливим чинником виникнення загрози даним виступає людський чинник, оскільки близько 16% випадків порушення інформаційної безпеки компаній стають можливими внаслідок утрати співробітниками мобільних при-

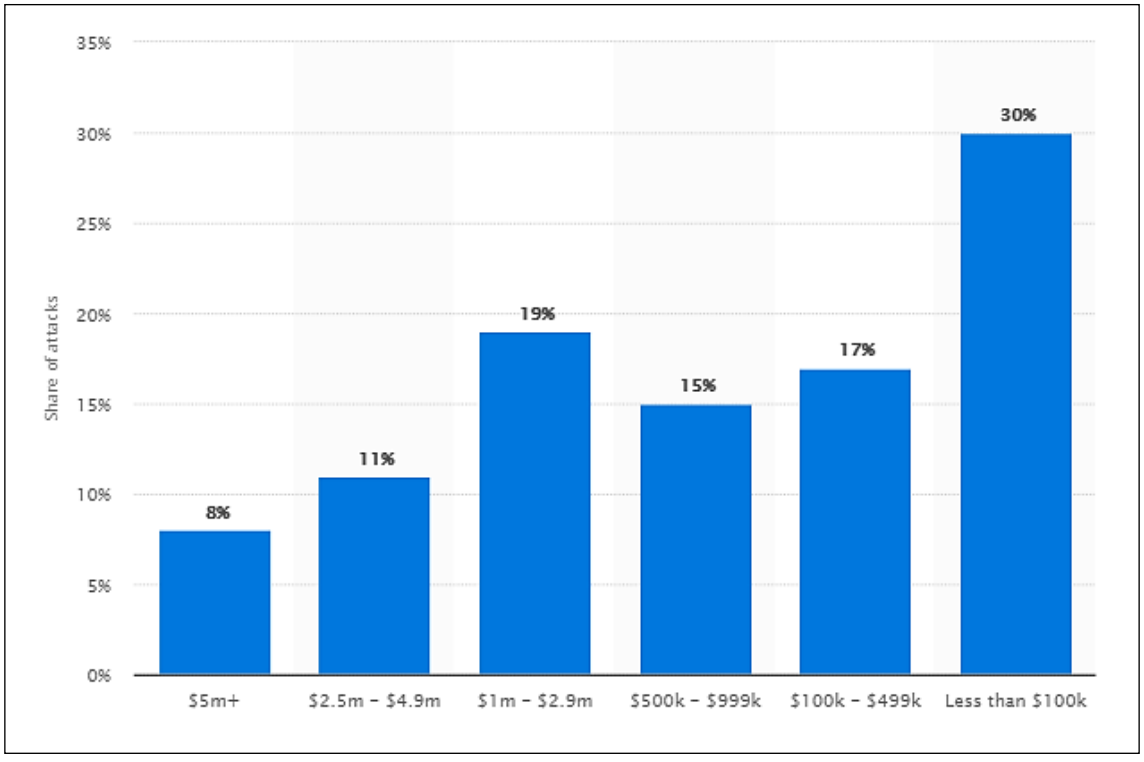

Рис. 1. Середній економічний збиток від кібератак на підприємства в усьому світі станом на квітень 2018 р. (дол. США) [3]

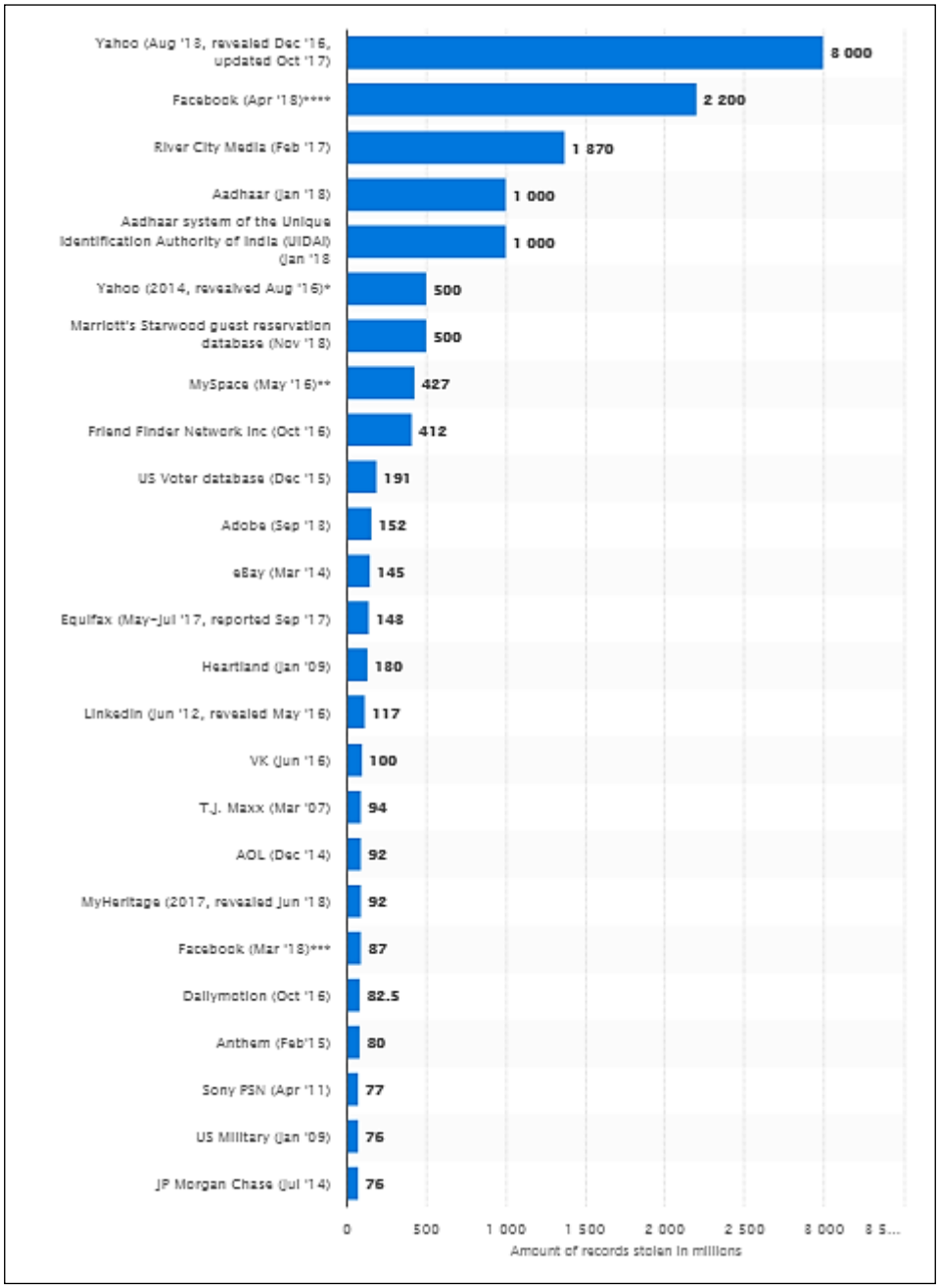

Рис. 2. Розподіл компаній за найбільшою кількістю скомпрометованих записів персональних даних станом на листопад 2018 р. [3]

строїв, що мають доступ до корпоративних баз даних, містять відповідну секретну інформацію про діяльність компаній або зберігають ключі та паролі доступу до певних ресурсів.

В окреслених умовах керівництву компаній необхідно розробити ефективну стратегію інформаційної безпеки, що повинна містити такі етапи:

1. Визначення місця інформаційної безпеки в системі забезпечення функціонування компанії. На цьому етапі необхідно врахувати ключові особливості функціонування конкретної компанії, її структурних підрозділів, наявні ресурси та можливості. Особливо актуальним це завдання є для ТНК, які мають філії у різних регіонах світу. У цьому разі необхідно застосувати індивідуальний підхід до кожної компанії в рамках нормативно-правових актів держави, що дасть змогу побудувати ефективну систему інформаційного захисту за умови оптимального використання наявних ресурсів.

2. Виявлення наявних ризиків. На основі індивідуальних ризиків компанії та з урахуванням її специфічних потреб необхідно провести комплексний аналіз можливих загроз. Під час побудови системи кібербезпеки компанії виявлені у ході дослідження ризики необхідно врахувати, що дасть можливість забезпечити високий рівень інформаційної безпеки.

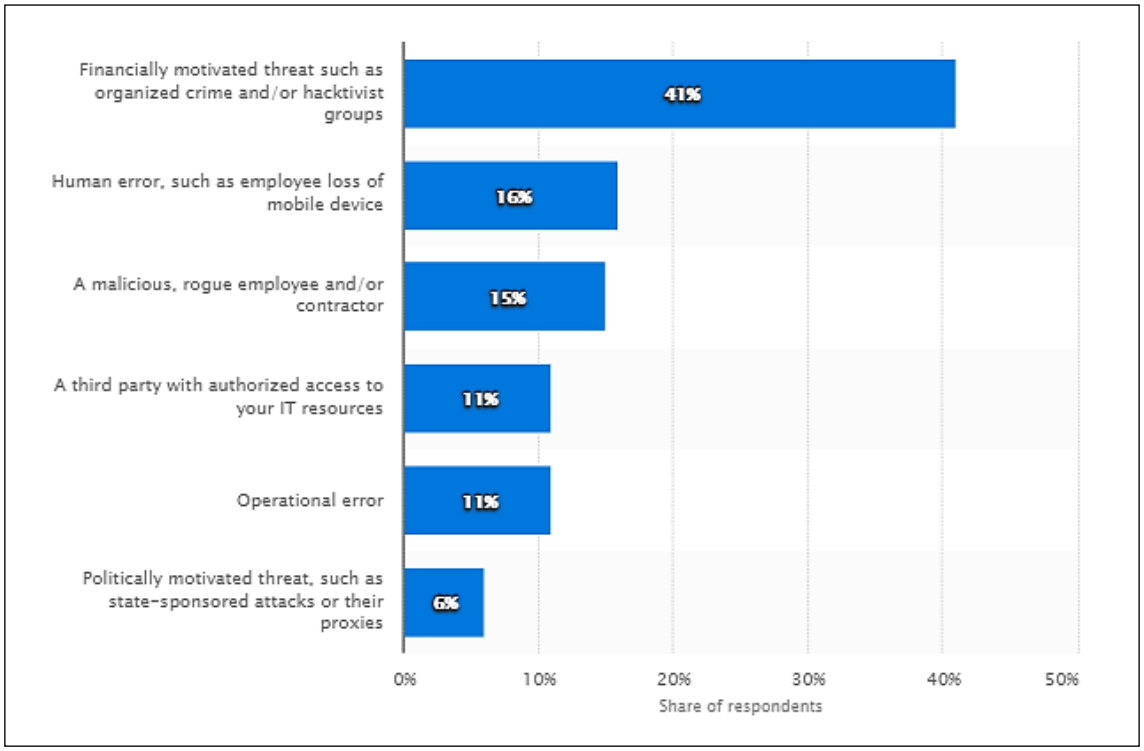

Рис. 3. Результати опитування керівників міжнародних компаній стосовно ризику кібератак у розподілі за основними напрямами станом на лютий 2018 р. [3]

3. Розроблення та запровадження політики безпеки. На основі чинного законодавства та передового досвіду у сфері інформаційної безпеки необхідно розробити та запровадити систему інформаційного захисту. Інноваційна система передбачає не лише використання новітніх підходів та інструментів, а й використання елементів попередньої системи інформаційної безпеки, які є актуальними в сучасних умовах та довели свою ефективність і доцільність використання у майбутньому.

4. Управління безпекою. Важливу роль у забезпеченні ефективного функціонування системи інформаційної безпеки відіграють працівники різних ланок управління. На рівні керівництва уповноважена особа відповідає за розроблення та виконання стратегічних заходів щодо забезпечення кібербезпеки компаній. На рівні системних адміністраторів посадові обов'язки передбачають тестування та перевірку системи, а також виконання щоденних адміністративних заходів. Керівники вищих рівнів контролюють виконання підлеглими посадових обов'язків щодо забезпечення інформаційної безпеки в компаніях.

5. Програмний захист інформації. На цьому етапі проводиться класифікація потенційних загроз комп'ютерному програмному забезпеченню за умови використання шкідливого софту. На основі отриманих результатів створюється або вдосконалюється система кібербезпеки від вірусів та іншого шкідливого програмного забезпечення.

6. Фізичний захист інформаційної системи. Поряд із боротьбою зі шкідливим програмним забезпеченням необхідно розробити комплекс заходів стосовно мінімізації ризиків пошкодження або знищення комп'ютерного обладнання, передусім йдеться про сервери, які займаються обробкою та збереженням відповідної інформації.

7. Створення системи доступу. Відповідно до рівня доступу до інформації в компанії кожній із категорій користувачів надаються різні права для роботи з даними. У цьому разі можуть використовуватися різноманітні стратегії налаштування прав доступу до інформації або запобігання щодо її використання [4–7].

Висновки з цього дослідження і перспективи подальших розвідок у даномунапрямку. Отже, компаніям потрібно приділяти значну увагу питанням захисту інформації, яка генерується в процесі їхньої діяльності. Необхідно мінімізувати ризики втрати даних, що пов'язані як безпосередньо з діяльністю установ, так і з приватним життям усіх учасників економічного процесу. Безперервна еволюція шкідливих програм передбачає постійне вдосконалення захисту даних. Головною метою компанії є розроблення дієвої стратегії, яка дасть змогу оптимізувати її діяльність, у тому числі й завдяки побудові ефективної системи захисту інформації. Компаніям для досягнення поставленої мети необхідно витрачати відповідні фінансові ресурси, що відповідатимуть можливим економічним збиткам унаслідок утрати або пошкодження відповідних даних.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Чубукова О.Ю., Раллє Н.В. Складові інноваційної економіки – освіта, технологічні уклади, когнітивні технології. Науковий вісник Полісся. 2016. № 3(7). С. 130–133.
2. Rzepka A., Ślusarczyk B. Correlation and dependence between: Business-Globalisation-Information Society and Global Society. International Journal of Management Invention. 2016. Vol. 5 Is. 1. ISSN 2319-8028s. 39-45.
3. Офіційний сайт Statista. URL: https://www.statista.com/.
4. Trends in cyber security of 2018. URL: https://www.fox-it.com/en/about-fox-it/corporate/news/trends-cyber-security-2018/.
5. State of cybersecurity 2018. URL: https://cybersecurity.isaca.org/state-of-cybersecurity.
6. IT Security Insights 2019. URL: https://it-security-insights-2019.confetti.events/.
7. Information and cyber security: 5 trends to watch in 2018. URL: https://www.pluralsight.com/resource-center/guides/info-cyber-security/thank-you.

REFERENCES:

1. Chubukova O.Yu., Rallye N.V. (2016) Skladovi innovatsiynoyi ekonomiky – osvita, tekhnolohichni uklady, kohnityvni tekhnolohiyi [Components of innovative economy – education, technological way, cognitive technologies]. Naukovyy visnyk Polissya, vol. 3, no. 7, pp. 130-133.
2. Rzepka A., Ślusarczyk B., Correlation and dependence between: Business-Globalisation-Information Society and Global Society, International Journal of Management Invention, Volume 5 Issue 1, January 2016, ISSN 2319-8028s. 39-45.
3. Official site of Statista. Available at: https://www.statista.com/
4. Trends in cyber security of 2018. Available at: https://www.fox-it.com/en/about-fox-it/corporate/news/trends-cyber-security-2018/
5. STATE OF CYBERSECURITY 2018. Available at: https://cybersecurity.isaca.org/state-of-cybersecurity
6. IT Security Insights 2019. Available at: https://it-security-insights-2019.confetti.events/
7. Information and cyber security: 5 trends to watch in 2018. Available at: https://www.pluralsight.com/resource-center/guides/info-cyber-security/thank-you

Chubukova O.Yu.
Doctor of Economic Sciences, Professor,
Head of Economic Cybernetics and Marketing Department,
Kyiv National University of Technologies and Design

Ponomarenko I.V.
Candidate of Economic Sciences, Associate Professor,
Senior Lecturer at Economic Cybernetics and Marketing Department,
Kyiv National University of Technologies and Design

PECULIARITIES OF INFORMATION SECURITY IN MODERN CONDITIONS

The article presents the current situation regarding the implementation of cyberattacks on the world's companies. The main statistical information about losses from illegal actions with company information is given. It is determined the targeting of criminal gangs against illegal manipulations with these companies to obtain economic benefits. The importance of providing an effective information security system for companies is proved. The main stages of ensuring information security are presented, which should be contained in the company's respective strategy. These are:

1. Determination of the place of information security in the system of ensuring the operation of the company.

2. Detection of existing risks. On the basis of the company's individual tracks and taking into account its specific needs, it is necessary to conduct a comprehensive analysis of possible threats.

3. Development and implementation of security policy. On the basis of current legislation and best practices in the field of information security, it is necessary to develop and implement an information protection system.

4. Security management. The important role in ensuring the effective functioning of the information security system is played by the employees of different levels of management. At the level of the campaign, the authorized person is responsible for the development and implementation of strategic measures to ensure the cybersecurity of companies. At the level of system administrators, official duties include testing and checking the system, as well as performing daily administrative measures. Heads of higher levels control the performance of subordinate duties to provide information security in companies.

5. Software protection of information. At this stage, the classification of potential threats to computer software is provided under the condition of malicious software use.

6. Physical protection of the information system. Along with the fight against malicious software, it is necessary to develop a set of measures to minimize the risk of damage or destruction of computer equipment; first of all, it is about servers that deal with the processing and preservation of relevant information.

7. Creating an access system. In accordance with the level of access to information in the company, each category of user is given different rights to work with data. In this case, various strategies can be used to set up access rights to information or to prevent its use.