УДК 004. 239 **doi: 10.26906/SUNZ.2019.2.078**

Л. М. Дегтярьова[1], М. В. Мірошникова[2], С. В. Волошко[1]

[1] Полтавський національний технічний університет імені Юрія Кондратюка, Полтава, Україна,
[2] Східноукраїнський національний університет імені В. Даля, Сєвєродонецьк, Україна

АНАЛІЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

В статті виконаний аналіз пріоритетних елементів архітектури системи захисту інформації з позиції ефективності її роботи. Система включає в себе модулі для реєстрації, обліку та обмеження доступу з урахуванням затверджених норм та правил, шифрування інформації, що передається або зберігається, резервування інформаційних ресурсів та забезпечення цілісності. Проаналізовано основні компоненти забезпечення інформаційної безпеки, які здійснюють контроль ефективності проведених заходів та заходів, що вживаються щодо захисту інформації з використанням технічних засобів. Усі ці модулі доцільно використовувати як обов'язкові компоненти системи захисту інформації, хоча переважна більшість загроз для інформаційної системи може бути реалізована лише під час роботи обчислювальної системи. Система інформаційної безпеки є структурною одиницею інформаційної системи; це структурна, функціональна та організаційна складова, що відтворює архітектуру захищеної системи. Безперервність контролю необхідна для постійного захисту всіх елементів системи. Вона повинна бути надійною і працювати як в активному, так і в пасивному стані інформаційної системи. Підвищення безпеки будь-якого об'єкта може бути досягнуто за допомогою багаторівневої і багатокомпонентної конструкції системи захисту. У цьому випадку реалізація будь-якої загрози зможе впливати на об'єкт, що охороняється, лише якщо всі встановлені рівні захисту будуть подолані, з урахуванням всього комплексу вимог захисту та факторів, що впливають на захист.

Ключові слова: інформаційна безпека, система захисту інформації, інформаційні загрози, несанкціонований доступ, оптимізація архітектури, контроль доступу.

Вступ

Постановка проблеми. Використання новітніх інформаційних технологій, автоматизованих систем управління та інформаційно-аналітичних систем тобто тих систем, які мають безпосередній вплив на оборону країни, безпеку життєдіяльності людини, економіку, транспортну логістику, науку тощо, відображають рівень розвитку інформаційного суспільства взагалі і в Україні зокрема. Робота з інформацією, а саме її збір, фіксація, перетворення, зчитування, передача, зберігання та знищення – це ті процеси, які використовуючи конгломерат апаратних і програмних засобів та інформаційно-телекомунікаційних мереж, потребує високого рівня інформаційної безпеки

Мета статті – відобразити можливу структуру системи інформаційної безпеки або систем захисту інформації (СЗІ), яка здатна запобігати нанесенню шкоди через неповноту інформації, її несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки комп'ютерних систем вже досить давно стали предметом особливої уваги не тільки вузького кола спеціалістів, але й великої кількості розробників і користувачів сучасних інформаційних технологій, автоматизованих систем управління та інформаційно-аналітичних систем. Розвиток інформаційних технологій в сфері інженерних і транспортних мереж потребує інтеграції різноманітних спеціалізованих програмних і апаратних компонентів і тому комплексне вирішення завдань захисту даних диктується не тільки доцільністю запобігання максимальному спектру загроз інформаційній безпеці. Без реалізації комплексного підходу до вирішення завдання захисту інформації неможливо ефективно вирішити жодної локального завдання захисту. Цій проблемі присвячені роботи фахівців у сфері інформаційної безпеки Хорошка В.О., Кормич Б.А., Шорошев В.В., Чекатков А.О., Степанов Є.О., Корнєєв І.К., Рибальський О.В., тощо.

Спираючись на фундаментальні поняття, положення і висновки досліджень можна стверджувати, що Інформаційна безпека є складним, системним і багаторівневим фактором, на стан і перспективи розвитку якого мають безпосередній вплив захист інформаційного простору; захист інформації з обмеженим доступом; захист інформаційних ресурсів [1–5]. При цьому під безпекою інформації розуміють такий стан інформації, яку зберігають, обробляють і передають, при якому неможливе випадкове навмисне розкриття, зміна або знищення даних [4].

Результати досліджень в області інформаційної безпеки показали, що безпека інформації комп'ютерних систем забезпечується та підтримується комплексом апаратно-програмних засобів і повинна бути захищена від будь-яких атак, але в той же самий час існує наявність різних помилок, від яких страждають і самі засоби захисту. Дана обставина дає необхідність урахування багатьох чинників, серед яких повинні бути навмисне порушення цілісності, можливість втрати або часткового спотворення службової інформації, яка може трапиться в результаті відмов апаратних або програмних засобів системи захисту інформації [6].

Захист інформації, яка обробляється в інформаційно-телекомунікаційних системах (ІТС), полягає в створенні і підтримці в активному та дієздатному стані заходів - як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки інформації, що зберігається в ІС або обертається в ІТС в цілому, тобто тако-

го стану, яке забезпечує збереження заданих властивостей інформації і ІТС, яка її обробляє.

Основна частина

Процес інформатизації сучасного світу на сьогоднішній день визначає рівень інформаційної безпеки спираючись на необхідність різнопланового захисту інформації, незалежно від місця знаходження її носіїв.

Широке використання спеціалізованих і глобальних інформаційних систем (ІС) в органах управління, структурах охорони здоров'я, на транспорті та у сфері державотворення дають можливість накопичувати і передавати величезні обсяги цінної інформації [5–8]. Але, в той же час, саме широке використання ІС робить ці системи вразливими для неконтрольованого доступу до інформації, що захищається, зростають ризики і небезпеки несанкціонованих впливів на інформацію в цих системах.

До факторів уразливостей ІС належить відносно велика величина небезпеки внутрішніх інформаційних загроз, широке використання кримінальними структурами пристроїв таємного отримання інформації, зростання числа злочинів у сфері комп'ютерної інформації.

Одним з основних компонентів забезпечення інформаційної безпеки є контроль ефективності проведених заходів та заходів, що вживаються щодо захисту інформації з використанням технічних засобів, оскільки сьогодні неможливо своєчасно прогнозувати і виявляти загрози, достовірно оцінювати небезпеку і вживати адекватних заходів щодо їх усунення.

При реалізації ефективного захисту конфіденційних даних засоби захисту інформації від несанкціонованого доступу та засоби захисту даних повинні розглядатися як засоби, що взаємодоповнюють одне одному.

Система захисту інформації (СЗ) визначається як сукупність всіх засобів, методів і заходів, які потенційно можуть бути використані для вирішення певних завдань із захисту об’єктів, що входять до складу ІС [5].

СЗІ повинна відповідати ряду вимог, найважливіші з яких представлено на рис. 1.

Вимоги до СЗІ	Сукупності завдань із захисту інформації та пропозиції щодо їх вирішення
	Забезпечення всіх вимог захисту
	Мінімальні перешкоди для користувача
	Зручність для персоналу, що обслуговує систему захисту
	Мінімізація витрат на систему захисту
	Максимальне використання серійних засобів
	Комплексне використання засобів
	Оптимізація архітектури
	Структурованість всіх компонентів
	Простота експлуатації

Рис. 1. Єдина концепція захисту інформації

Крім того, однією з вимог до складу і функціональним можливостям систем захисту інформації є вимога адаптованості: спроможності пристосування до зміні структури або умов функціонування об’єктів ІС.

Сама по собі система захисту інформації має дуалістичну властивість: з одного боку СЗІ є невід’ємною складовою системи обробки інформації і має здійснювати захист всієї сукупності об’єктів, що входять до складу ІС, а з іншого – СЗІ повинна бути автономною, незалежною від інших підсистем.

СЗІ повинна контролювати всі процедури автоматизованої обробки інформації, що циркулює в ІС, і результати контролю (основного і проміжних) повинні реєструватися в спеціальних реєстраційних журналах з фіксованим періодом часу перевірки.

Оскільки СЗІ є структурною одиницею ІС, тому вона являє собою структурну, функціональну та організаційну побудову, яка відтворює архітектуру системи, що вимагає захисту. Один з варіантів можливої архітектури представлено на рис. 2.

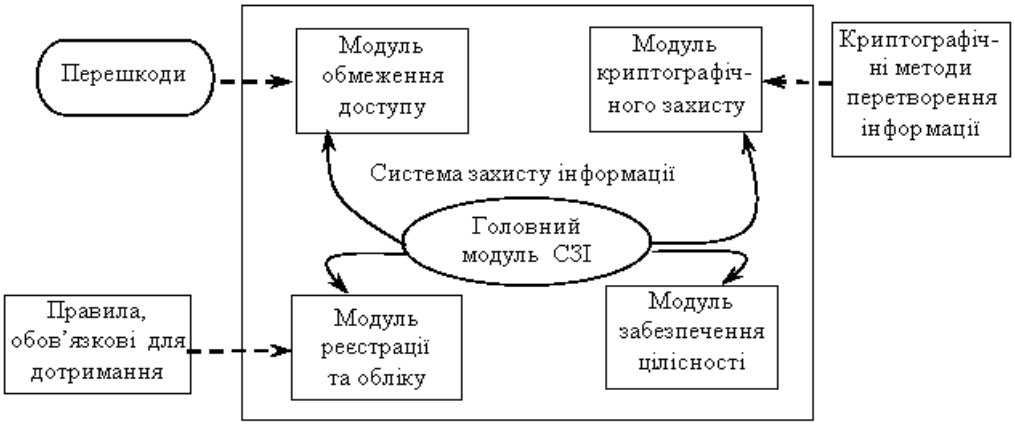

Рис. 2. Архітектурна побудова системи захисту інформації

Головний модуль системи захисту інформації призначений для об'єднання всіх модулів, що входять до складу СЗІ в єдину цілісну систему, для організації її функціонування. Головний модуль може включати організаційні (група співробітників спеціально виділених для забезпечення захисту інформації згідно розроблених правил та нормативної бази, які регламентують виконання цих функцій службою

захисту інформації) та технічні складові (сукупність технічних засобів СЗІ, відображення їх стану, контролю доступу до них, управління їх включенням тощо).

До функцій головного модулю системи захисту інформації належать:

організація і забезпечення перевірок коректності функціонування СЗІ;

блокування безконтрольного і несанкціонованого доступу до носіїв конфіденційної інформації або реагування при попередженні про спробу доступу;

управління потоками конфіденційної інформації;

контроль за виконанням вимог шифрування інформації і управління ключами шифрування;

контроль за періодичністю резервування інформаційних ресурсів;

визначення способу їх знищення після закінчення терміну придатності або застарівання інформації;

забезпечення недоступності засобів управління доступом з боку користувачів з метою їх зміни або вимкнення;

реєстрація всіх процесів, що відбуваються при функціонуванні системи; реєстрація даних для аналізу оцінки рівня безпеки об'єкта.

Модуль обмеження доступу призначений виконувати функції ідентифікації, автентифікації і контролю доступу користувачів і процесів до системи, серверу, мереж та каналів зв'язку; периферійних пристроїв, програм, дисків та файлів-носіїв конфіденційної інформації. Виходячи з перерахованих функцій і залежно від типу систем захисту до складу модуля обмеження доступу можуть входити наступні компоненти:

контролери, що відповідають для обмеження доступу;

ідентифікатори (безконтактні та контактні карти, електронні ключі, брелоки);

кардрідери різних рівнів складності (до їх складу належать і кардрідери для зчитування біометричних даних);

виконавчі пристрої, що обмежують або надають доступ до різних зон контрольованої території або об'єкта.

Контролер зберігає коди ідентифікаторів зі списком прав доступу кожного з власників ідентифікатора у власній незалежній пам'яті. У випадку використання мережевого зв’язку, контролер об'єднується в єдину систему з іншими контролерами і комп'ютером для можливості централізованого контролю і управління. У такому випадку рішення про надання доступу може прийматися як контролером, так і програмним забезпеченням головного комп'ютера.

При використання інтелектуальних IP-контролерів є можливість, крім функції контролю доступу, інтегрувати контролер з системами відеоспостереження, охоронною і пожежною сигналізацією. Контролер може мати додаткові цифрові входи для підключення різних датчиків, і додаткові силові виходи для управління елементами системи безпеки. На базі таких контролерів будуються системи доступу з забороною повторного проходу, реалізовується логіка роботи шлюзових кабін, записується відео події проходу, а також настроюються різні реакції інтегрованої системи безпеки на події в системах контролю та керування доступом, що входять до складу об’єктів ІС.

Ідентифікатор – це певне ім’я, яке дозволяє звернутись до об'єкта або ознака, яка цілком визначає сутність, в наперед визначеному просторі. Ідентифікатор, як унікальний параметр, дозволяє суб'єктові (користувачу або процесу, який діє від імені певного користувача) повідомити своє ім'я і повинен завжди мати сталі характеристики, а саме: розглядатися як неподільна (атомарна) номінативна одиниця; вказувати тільки на одну сутність; може існувати лише в одному адресному просторі.

В якості компонентів, що входять до модулю обмеження доступу можна додати мережеві сенсори, які призначені для спостерігання за мережевою активністю і збирають інформацію про події безпеки, які відбуваються в мережі. Обмеження доступу до ресурсів системи в певні інтервали часу часто зустрічається в інфокомунікаційних мережах, коли між користувачем і сервером (або групою серверів) знаходиться система захисту інформації (або її апаратна частина – супервізор). Вона і визначає розміри тимчасових інтервалів, протягом яких користувач має доступ до ресурсів. З функціонального погляду вони є пакетними аналізаторами, які декодують пакети з мережевого трафіку, здійснюють попередню фільтрацію до протоколів і передають отримані пакети детектору для подальшого аналізу. Пакетні аналізатори поділяються на два основних типи, а саме: системні (host-sensors) і мережеві (network-sensors) сенсори. Host-sensors здійснюють моніторинг стану системи, network-sensors досліджують зовнішні впливи на неї.

Модель обмеження доступу, реагуючи на спроби несанкціонованих дій, повинна виконати одну з процедур, залежно від засобів та методів втручання: переривання обробки даних, які захищаються; знищення інформації, яка може стати доступною внаслідок виявлених несанкціонованих впливів; термінове повідомлення про небезпечну ситуацію, що склалася, служби, яка відповідає за стан інформаційної безпеки; вживання заходів для виявлення порушника або/та усунення небезпеки.

Модуль, який призначений для криптографічного захисту, забезпечує цілісність і конфіденційність збереженої інформації на різного виду носіях та інформації, яка може бути передана по каналах зв'язку; забезпечення автентифікації джерела даних та приховування змісту конфіденційних повідомлень.

Серед можливих модулів, що входять до складу СЗІ, модуль забезпечення цілісності є обов’язковим та одним з найважливіших. До складу його функцій можуть входити засоби і методи для забезпечення адміністрування захисту інформації; відновлення СЗІ при можливих збоях; періодичне тестування функцій системи захисту персональних даних. Загрози порушення цілісності існують на всіх рівнях інформаційної системи: загрози цілісності

(достовірності) інформації або носія інформації (знищення носія і інформації, що зберігається на ньому); загрози цілісності програмного середовища та апаратної конфігурації інформаційної системи; загрози цілісності приміщення, що підлягає, будівлі, прилеглої території і т.д.

Модуль реєстрації та обліку використовуючи засоби реєстрації та обліку подій/ресурсів із зазначенням часу та учасника подій, відповідає за збір даних про події, що відбуваються в інформаційній системі, фіксування дати та часу друкування документу та кількості його друкованих копій; контроль та фіксація інформації про передачу даних у вигляді пакетів або повідомлень по лініях і каналах зв'язку. Реєстрація може здійснюватись за допомогою засобів ручного або автоматичного ведення журналу і формування підсумкових звітів роботи користувачів та обладнання за обраними параметрам, які повинні бути попередньо зареєстровані. Даний модуль необхідний для виявлення, запису та аналізу подій, пов'язаних із забезпеченням безпеки інформації, не дивлячись на те, що безпосередньо для запобігання порушенням безпеки цей модуль не використовується.

Ведення реєстраційних журналів (протоколів) системи захисту полягає (у випадку автоматичного ведення) в реєстрації спеціальними програмними засобами такої інформації:

час активації та деактивації системи захисту ресурсів активної ОС;

інформація про будь-яке намагання або вдалі спроби входу в ОС;

характер, час та результати реагування системи захисту на сигнали про намагання здійснити несанкціоновані дії;

відомості про початок та закінчення сеансів роботи користувачів;

інформація про всі запити на доступ до ресурсів та даних, які захищаються;

відомості про затримку та відмови у роботі програмно-апаратних засобів і результати регенерації;

інформація, яка пов’язана з запуском та закінченням роботи програм, з відкриттям, зміною та закриттям файлів тощо).

При виконанні проміжного контролю за коректним функціонуванням системи захисту інформації мають відбуватись перевірки:

апаратних засобів – за допомогою тестових програм;

програмних засобів − перевірка на цілісність та за іншими ідентифікуючими ознаками;

фізичних осіб – за допомогою організаційних заходів;

база даних еталонних та зразкових параметрів або даних, що забезпечує своєчасну видачу еталонних даних у випадку, якщо доступ до них здійснюється іншими компонентами системи захисту;

реєстраційних журналів − на цілісність та захищеність згідно з встановленими правилами та нормами;

інформація, яка захищається, − програмно на цілісність та захищеність;

організаційні засоби − проводиться співробітниками служб захисту.

Всі ці модулі доцільно використати в якості обов’язкових складових системи захисту інформації, але слід зазначити, що переважна більшість погроз інформаційній системі можуть бути реалізовані тільки в процесі функціонування обчислювальних системи.

Висновки

Інформація є основною складовою інформаційних систем різного призначення, в першу чергу автоматизованих систем управління, які мають можливість широкого застосування засобів обчислювальної техніки, периферійних пристроїв та засобів інфокомунікаційних мереж.

В інформаційних системах автоматизованих систем управління будь-якого призначення: в сферах державного управління, військової сфери, банківської діяльності, управління транспортними засобами тощо, постійно зростає обсяг та цінність стратегічної та конфіденційної інформації, яка використовується і передається по інфокомунікаційних мережах, тому велике значення мають швидкість та інформаційна надійність передачі даних, які визначають ефективність інформаційних систем.

Разом з тим зростає кількість інформації з обмеженим доступом, оскільки у сучасному суспільстві інформація набуває нового статусу: є гарантом успішної діяльності організації, або використовується як засіб інформаційної війни, тому актуальною проблемою є створення методології, концепції захисту інформації в інформаційних системах, її облік, обробка і зберігання та впровадження елементів архітектури систем захисту інформації в загальну інформаційну систему в якості обов’язкової складової.

Головний модуль системи захисту інформації має забезпечувати безперервне управління підпорядкованими йому модулями безпосереднього захисту об’єктів та функцій, розподілених по всіх структурних компонентах ІС, пов'язаних із зберіганням, обробкою та передачею інформації структурним елементам обчислювальної мережі, центрам зв'язку і комутації, сховищам інформаційних носіїв та інш. Безперервність управління необхідна для безперебійного захисту всіх елементів системи. Він має бути надійним і діяти безперебійно, як в активному, так і в пасивному стані ІС.

Значного підвищення безпеки будь-якого об'єкта можна досягти шляхом багаторівневої та багатокомпонентної побудови системи захисту. В цьому випадку реалізація будь-якої загрози зможе впливати на об'єкт, який захищається, тільки у разі подолання всіх встановлених рівнів захисту, при цьому враховується вся сукупність вимог до захисту і чинників, які впливають на захист. Це дозволить забезпечити необхідну безпеку інформації і процесу її обробки в обчислювальних системах.

Вирішуючи задачу захисту інформації, необхідно враховувати, що в загальному випадку захист полягає не тільки в протидії викраденню конфіденційної інформації, але і в забезпеченні її доступності і цілісності.

СПИСОК ЛІТЕРАТУРИ

1. М.М. Присяжнюк, Бєлашевич Я.С. Інформаційна безпека України в сучасних умовах/ Військово-спеціальні науки, №30 (1) − К.: Вісник Київського національного університету імені Тараса Шевченка, 2013. − с. 37-41.
2. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. – М.: ИНФРА-М, 2001. – 304 с.
3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібнік. – К.:Кондор, 2004. – 384 с.
4. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации – К.: Юниор, 2003. – 504 с.
5. Семкин С.Н., Беляков Э.В., Гребенев С.В. и др. Основы организационного обеспечения информационной безопасности объектов информатизации − М.: Издательство "Гелиос АРВ", 2005. − 186 с.
6. Degtyareva L., Miroshnykova M. The problems of the security of information transport and logistics systems/ // Theses of international scientific and practical conference “Globalization of scientific and educational space. Innovations of transport. Problems, experience, prospects”, May 2018, Italy. – С. 32-34.
7. Безштанько В. Аналіз існуючих програмних засобів та методик оцінки стану інформаційної безпеки організації // Бизнес и безопасность. – 2007. – №1. – С. 32-35.
8. Дегтярьова Л.М. Аналіз структури та використання інформаційної технології обробки даних // Вісник Східноукраїнського нац. університету ім. В. Даля. – Луганськ, СНУ ім. В. Даля, 2013. – №6 (195), ч. 1. – С. 18-20.
9. Amin Salih M., Yuvaraj D., Sivaram M., Porkodi V. Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol. *International Journal of Advanced Research in Computer Science*. Vol. 9, No 6. P. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
10. Porkodi V., Sivaram M., Mohammed A.S., Manikandan V. Survey on White-Box Attacks and Solutions. Asian Journal of Computer Science and Technology. Vol. 7, Is. 3. pp. 28–32.
11. Manikandan V, Porkodi V, Mohammed AS, Sivaram M, “Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering”, ICTACT Journal on Soft Computing, Volume 9, Issue 1, 2018, pp.1813-1816. DOI: 10.21917/ijsc.2018.0252
12. Комплексные системы защиты информации предприятия: учебное пособие / В.Т. Еременко, М.Ю. Рытов, О.М. Голембиовская, П.Н. Рязанцев. – Орел: ФГБОУ ВО «Орловский государственный университет имени И.С. Тургенева», 2016. – 116 с.

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв,
Харківський національний університет імені В.Н. Каразіна, Харків
Received (Надійшла) 11.02.2019
Accepted for publication (Прийнята до друку) 27.03.2019

Анализ структуры системы защиты информации

Л. Н. Дегтярева, М. В. Мирошникова, С. В. Волошко

В статье выполнен анализ приоритетных элементов архитектуры системы защиты информации с позиции эффективности ее работы. Система включает в себя модули для регистрации, учета и ограничения доступа на базе утвержденных норм и правил, шифрование информации, передаваемой или сохраняемой, резервирование информационных ресурсов и обеспечения целостности. Проанализированы основные компоненты обеспечения информационной безопасности, осуществляющие контроль эффективности проводимых мероприятий и мер, принимаемых по защите информации с использованием технических средств. Все эти модули целесообразно использовать как обязательные компоненты системы защиты информации, хотя подавляющее большинство угроз для информационной системы может быть реализовано только при работе вычислительной системы. Система информационной безопасности является структурной единицей информационной системы; это структурная, функциональная и организационная составляющая, воспроизводит архитектуру защищенной системы. Непрерывность контроля необходима для постоянной защиты всех элементов системы. Она должна быть надежной и работать как в активном, так и в пассивном состоянии информационной системы. Повышение безопасности любого объекта может быть достигнуто с помощью многоуровневой и многокомпонентной конструкции системы защиты. В этом случае реализация любой угрозы сможет влиять на охраняемый объект, только если все установленные уровни защиты будут преодолены, с учетом всего комплекса требований защиты и факторов, влияющих на защиту.

Ключевые слова: информационная безопасность, система защиты информации, информационные угрозы, несанкционированный доступ, оптимизация архитектуры, контроль доступа.

Analysis of the structure of the information security system

L. Degtyareva, M. Miroshnykova, S. Voloshko

The article analyzes the priority elements of the information protection system architecture from the standpoint of the effectiveness of its work. The system includes modules for registering, recording and restricting access based on approved norms and rules, encrypting information transmitted or stored, reserving information resources and ensuring integrity. Analyzed the main components of information security, monitoring the effectiveness of measures taken and measures taken to protect information using technical means. It is advisable to use all these modules as mandatory components of an information protection system, although the vast majority of threats to an information system can be implemented only during the operation of a computing system. The information security system is a structural unit of an information system; therefore, it is a structural, functional and organizational component that reproduces the architecture of the protected system. Continuity of control is necessary for the continuous protection of all elements of the system. It must be reliable and operate smoothly, both in the active and in the passive state of the information system. Enhance the security of any object can be achieved through a multi-level and multi-component construction of the protection system. In this case, the implementation of any threat will be able to influence the protected object only if all established protection levels are overcome, taking into account the entire set of protection requirements and factors affecting protection.

Keywords: information security, information protection system, information threats, unauthorized access, architecture optimization, access control.