МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук і технологій

Кафедра прикладної математики та інформатики

ПОЯСНЮВАЛЬНА ЗАПИСКА

до курсового проекту з дисципліни "Безпека програм та даних"

на тему: "Аналіз ризиків інформаційної безпеки та розробка   
комплексу заходів захисту програм та даних"

Розробник:

студент групи ІПЗ-13

Лисенко А.С.

Керівники:

к.т.н., доц. каф. ПМІ

Маслова Н.О.

асистент каф. ПМІ

Скрипник Т.

Покровськ 2016

# Реферат

Пояснювальна записка курсового проекту містить 57 сторінки, 7 малюнків, 2 додатки.

Об'єктом дослідження даного курсового проекту є забезпечення інформаційної безпеки програм та даних, розміщених на ПК студента, що взаємодіє у локальній мережі навчального закладу.

Метою роботи є аналіз ризиків та розробка комплексу заходів підвищення безпеки ПК користувача й взаємозв'язаних з ним пристроїв.

Головна задача - здобуття навичок виділення загроз інформаційної безпеки, розрахунок ризиків з застосуванням інструментальних пакетів та формування плану їх мінімізації.

Результатами виконання курсового проекту є:

* аналіз та розрахунок ризиків інформаційної безпеки;
* план зниження ризиків;
* пропозиції щодо застосування криптографічного захисту.

В рамках курсового проекту було реалізовано програму, яка виконує шифрування тектсту за допомомогою алгоритмім DES з довжиною ключа 64 біт та AES з довжинами ключів 128 біт, 196 біт і 256 біт.

ІНФОРМАЦІЙНА СТРУКТУРА (ІС), БЕЗПЕКА ПРОГРАМ ТА ДАНИХ, АЛГОРИТМ, цілісність інформації, АНАЛІЗ РИЗИКІВ, об'єкт

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ВСТУП  Курсовий проект за курсом «Безпека програм та даних» має сприяти відточуванню навичок захисту програм та даних, розміщених на персональних комп'ютерах та розробку комплексу заходів з підвищення рівня цього захисту. Виконання курсового проекту на тему «Аналіз ризиків інформаційної безпеки та розробка комплексу заходів захисту програм та даних» допомагає набуттю вмінь обирати та застосувати криптографічні алгоритми, виконувати систематизацію ризиків, проводити їх оцінку та мінімізацію. Курсове проектування дозволить сформувати навички з застосування криптографічних бібліотек, розробку й оцінювання якості комплексу контрзаходів, а також налагоджування обчислювальних процедур шифрування даних.  Об'єктом дослідження даного курсового проекту є забезпечення інформаційної безпеки програм та даних, розміщених на ПК студента, що взаємодіє у локальній мережі навчального закладу.  Метою роботи є аналіз ризиків та розробка комплексу заходів підвищення безпеки ПК користувача й взаємозв'язаних з ним пристроїв.  Головна задача - здобуття навичок виділення загроз інформаційної безпеки, розрахунок ризиків з застосуванням інструментальних пакетів та формування плану їх мінімізації.  Результатами виконання курсового проекту повинно бути:  - аналіз та розрахунок ризиків інформаційної безпеки;  - план зниження ризиків;  - пропозиції щодо застосування криптографічного захисту.  1 ПІДСТАВИ ДЛЯ РОЗРОБКИ  Курсовий проект виконується на підставі навчального плану підготовки студентів за освітньо-кваліфікаційним рівнем «бакалавр з програмної інженерії» та «Технічного завдання до курсового проекту» за дисципліною «Безпека програм та даних» для студентів, що отримують освіту в галузі знань 0501 «Інформатика та обчислювальна техніка», напряму підготовки 6.050103 «Інженерія програмного забезпечення».  2 ПРИЗНАЧЕННЯ РОЗРОБКИ  Розробка орієнтована на закріплення практичних навичок з розрахунку ризиків, аналізу та оцінювання рівня захисту програм та даних, застосування криптографічних бібліотек, розробки і програмної реалізації алгоритмів захисту, що рекомендовано за переліком контрзаходів, обраних в процесі роботи однієї з систем аналізу ризиків.  Під час виконання курсової роботи студент повинен систематизувати активи об’єкту захисту, сформувати перелік погроз інформаційної безпеки, оцінити рівень існуючих та можливих ризиків, пропонувати перелік контрзаходів, які повинні привести до зниження сумарного рівня ризиків та оцінити ступінь цього зниження. Результатом розробки повинна стати програмна реалізація одного з криптографічних алгоритмів, рекомендації щодо їх застосування з підтвердженням ефективності пропонованих дій з захисту програм та даних. При виконанні курсового проекту має бути застосована одна з систем розрахунку ризиків інформаційної безпеки (CORAS, CRAMM, RiskWatch, Digital Security або ін.). Загальний аналіз рівня захищеності програм та даних повинен виконуватися згідно вітчизняних та міжнародних стандартів інформаційної безпеки.  3 ВИМОГИ ДО ФУНКЦІОНУВАННЯ ПРОГРАМНОЇ РОЗРОБКИ  3.1 Вимоги до надійності  Програмний виріб повинен:  1) бути ефективним по швидкодії;  2) застосовувати ключі безпеки, які гарантують стійкість криптографічного алгоритму;  3) підвищувати рівень захищеності програм та даних;  4) багатократно виконувати шифрування та розшифрування блоків даних з отриманням ідентичних результатів;  3.2 Вимоги до складу й параметрів технічних засобів  Для функціонування програмного виробу необхідний персональний комп'ютер зі стандартним набором периферійних пристроїв (монітор, клавіатура, миша).  3.3 Вимоги до інформаційної й програмної сумісності  Курсова робота може бути виконана на будь-якій мові високого рівня з використанням криптографічних бібліотек (PyCripto, Cripto API, MCrypt, OpenSSL, Cryptography, Java Cryptography Extension JCE, Bouncy Castle, Cripto C++ або ін.), працювати в середовищі встановленої на ПК розробника операційної системи (переважно MS Windows), застосовувати системи оцінювання та розрахунку ризиків інформаційної безпеки.  4 СТАДІЇ Й ЕТАПИ РОЗРОБКИ   |  |  |  |  | | --- | --- | --- | --- | | № з/п | Назва етапів дипломної роботи | Строк виконання етапів роботи | Примітка | | 1 | Дослідження предметної області | 01.09.2016 – 15.09.2016 |  | | 2 | Вибір стандартів | 16.09.2016-30.09.2016 |  | | 3 | Дослідження існуючих методів захисту програм та даних | 01.10.2016 – 15.10.2016 |  | |  | Дослідження пакету «ГРИФ» | 16.10.2016 – 31.10.2016 |  | | 4 | Виділення та аналіз ризиків, складання плану аварійних засобів | 01.11.2016 – 15.11.2016 |  | | 5 | Розробка криптографічних алгоритмів | 16.11.2016 – 30.11.2016 |  | | 7 | Тестування алгоритмів | 01.12.2016– 10.12.2016 |  | | 11 | Написання ПЗ | 11.12.2016 – 11.12.2016 |  | | 12 | Захист курсової роботи | 21.12.2016 |  |   5 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ  Загальні вимоги  Загальними вимогами текстової частини студентської роботи є:  - чіткість і логічна послідовність викладу матеріалу;  - переконливість аргументації;  - стислість і точність формулювань, що виключають можливість суб'єктивного й неоднозначного тлумачення;  - конкретність викладу результатів виконання проведеної роботи;  - доказовість і обґрунтованість рекомендацій і пропозицій;  - єдність термінів у межах роботи і їхня відповідність установленим стандартам.  При викладі не допускається переписування загальних положень, а так само визначень із підручників, навчальних статей, посібників і інших джерел. При необхідності використання в текстовому документі матеріалів з літературних джерел, необхідно робити на них посилання по тексту.  Структурні частини текстового документа починають із нового аркуша, їх не нумерують. Заголовки структурних одиниць записуються по центру й прописними буквами; підрозділи з нового рядка й тільки перша буква прописна.  Сторінки нумеруються арабськими цифрами. Нумерація сторінок наскрізна по всьому текстовому документу й проставляється в правому верхньому куті сторінки. Титульний аркуш, реферат, лист завдання не нумеруються, але входять у загальне число сторінок.  При написанні пояснювальної записки використовується шрифт Times New Roman, розмір 14, накреслення Звичайний. Забороняється використовувати накреслення Курсив, Підкреслення й Напівжирний.  6. Рекомендований зміст пояснювальної записки  Вступ   1. Основна частина  * Опис інформаційних ресурсів; * Схема міжкомп'ютерної взаємодії; * Характеристика апаратного та програмного забезпечення; * Оцінювання рівня безпеки структури згідно стандартів.   2. Керування ризиками інформаційної безпеки   * Аналіз загроз інформаційної безпеки; * Класифікація джерел загроз; * Уразливості інформаційної структури; * Визначення ризиків інформаційної безпеки.   3. Процедури інформаційної безпеки   * + Законодавчі заходи   + Адміністративні заходи   + Процедурні заходи   + Програмно-технічні заходи:   - Засоби криптографічного захисту;  - Засоби розмежування доступу;  - Засоби мережевого екранування;  - Засоби антивірусного захисту та виявлення атак;  - Засоби захисту від спаму;  - Засоби контентного аналізу та виявлення закладок.  4. Розробка засобів захисту й аварійного плану.  - Захист від ненавмисних загроз;  - Захист від навмисних загроз.  5. Алгоритм криптографічного захисту програм та даних:  - призначення алгоритму та сфера застосування;  - схема функціонування;  - опис програмної розробки.  Висновки  Перелік застосованих джерел  Додаток А. Основні законодавчі акти у сфері інформаційної безпеки.  Додаток Б. Результати розрахунків за допомогою системи «ГРИФ»  Додаток В. Криптографічний алгоритм (програмний код)  Додаток Г. Результати застосування криптографічного захисту  7 ПОРЯДОК КОНТРОЛЮ Й ПРИЙОМУ  Курсовий проект виконується 15 тижнів. Пояснювальна записка до курсового проекту надається на перевірку викладачам не менш чим за 3 робочі дні до дати захисту.  Захист відбувається в присутності комісії в складі 2-3 чоловік і включає:  а) доповідь, що відбиває всі етапи проектування курсового проекту;  б) презентацію програми;  в) відповіді на запитання комісії. |

Варіант завдаННя

|  |  |  |
| --- | --- | --- |
| **вар** | **Состав інформаційної структури** | **Стандарти для оцінювання рівня безпеки** |
| 7 | ПК розробника, обмін розробками по мережі з трьома випадковими респондентами | Британський стандарт з інформаційної безпеки (BS 7799) |

9. Перелік РЕКОМЕНДОВАНИХ джерел

1. А.К. Плешков. Политика информационной безопасности «Газпромбанк» [Электронный ресурс]. — Электрон. дан.: 2009 — Режим доступа: <http://www.gazprombank.ru/upload/iblock/ee7/infibez.pdf> — Загл. с экрана. — Яз. рус.
2. Политика информационной безопасности [Электронный ресурс]. — Электрон. дан.: 2009 — Режим доступа: <http://securitypolicy.ru/index.php/Политика_информационной_безопасности_(финансовые_организации)> — Загл. с экрана. — Яз. рус.
3. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
4. Проектирование системы информационной безопасности [Электронный ресурс]. — Электрон. дан.: 2010 — Режим доступа: <http://www.bestreferat.ru/referat-141804.html> — Загл. с экрана. — Яз. рус.
5. Критерии определения безопасности компьютерных систем безопасности [Электронный ресурс]. — Электрон. дан.: 2012 — Режим доступа:http://ru.wikipedia.org/wiki/Критерии\_определения\_безопасности\_компьютерных\_систем — Загл. с экрана. — Яз. рус.
6. TCO, или Как управлять IT-затратами [Электронный ресурс]. — Электрон. дан.: 2001 — Режим доступа: http://www.management.com.ua/ims/ims023.html — Загл. с экрана. — Яз. рус.
7. Экономика информационной безопасности [Электронный ресурс]. — Электрон. дан.: 2007 — Режим доступа: <http://www.trn.ua/articles/2081/> — Загл. с экрана. — Яз. рус.
8. Астахов А. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. — 312 с. — ISBN 978-5-94074-574-7
9. [Нестеров](http://www.intuit.ru/lector/472.html) С.А. Управление рисками. Модель безопасности с полным перекрытием[Электронный ресурс]. — Электрон. дан.: 2003 — Режим доступа: <http://www.intuit.ru/department/itmngt/riskanms/1/> — Загл. с экрана. — Яз. рус.
10. Положение «О требованиях по обеспечению информационной безопасности в коммерческих банках Кыргызской Республики»  [Электронный ресурс]. — Электрон. дан.: 2003 — Режим доступа: <http://www.nbkr.kg/contout.jsp?item=103&lang=RUS&material=25990> — Загл. с экрана. — Яз. рус.
11. Шнайер, Брюс. Секреты и ложь. Безопасность данных в цифровом мире (Secrets and Lies: Digital Security in a Networked World ).: 2000г. ISBN 0-471-25311-1
12. Справочная, Закон Украины «О платежных системах и переводе средств в Украине» [Электронный ресурс]. — Электрон. дан.: 2001 — Режим доступа: http://www.trust.ua/news/56985-spravochnaya-zakon-ukrainy-o-platezhnyh-sistemah-i-perevode-sredstv-v-ukraine.html — Загл. с экрана. — Яз. рус.
13. Законодательство Украины в сфере защиты персональных данных и информационной безопасности » [Электронный ресурс]. — Электрон. дан.: 2001 — Режим доступа: http://www.uipdp.com/solutions/services/consulting/legislation/ua/ — Загл. с экрана. — Яз. рус.
14. Планирование мер обеспечения информационной безопасности [Электронный ресурс]. — Электрон. дан.: 2008 — Режим доступа: <http://www.sernam.ru/ss_33.php> — Загл. с экрана. — Яз. рус.
15. Закон Украины «Про банки і банківську діяльність» [Электронный ресурс]. — Электрон. дан.: 2002 — Режим доступа: <http://zakon1.rada.gov.ua/laws/show/2121-14> — Загл. с экрана. — Яз. рус.
16. Юрий Мельников, Алексей Теренин "Банковские технологии" [Электронный ресурс]. — Электрон. дан.: 2001 — Режим доступа: <http://citforum.univ.kiev.ua/security/articles/banks/> — Загл. с экрана. — Яз. рус.
17. Игнатьев В.А. И 266 Информационная безопасность современного

коммерческого предприятия: Монография. — Старый Оскол: ООО

«ТНТ», 2005. — 448 с. ISBN 5-94178-070-2

1. Защита сервера [Электронный ресурс]. — Электрон. дан.: 2009 — Режим доступа: <http://www.hackzone.ru/articles/view/id/8537/> — Загл. с экрана. — Яз. рус.
2. Шифруемся на лету при помощи TrueCrypt [Электронный ресурс]. — Электрон. дан.: 2008 — Режим доступа: <http://www.hackzone.ru/articles/view/id/8058/> — Загл. с экрана. — Яз. рус.
3. Обманываем взломщика[Электронный ресурс]. — Электрон. дан.: 2009 — Режим доступа <http://www.hackzone.ru/articles/view/id/2232/> — Загл. с экрана. — Яз. рус.

Оглавление

[Введение 1](#_Toc472106060)

[Концепция информационной безопасности 3](#_Toc472106061)

[1. Основные концептуальные положения системы защиты информации 3](#_Toc472106062)

[2. Концептуальная модель информационной безопасности 3](#_Toc472106063)

[3. Угрозы конфиденциальной информации 3](#_Toc472106064)

[4. Действия, приводящие к неправомерному овладению конфиденциальной информацией 3](#_Toc472106065)

[1.1 Основные концептуальные положения системы защиты информации. 5](#_Toc472106066)

[1.2. Концептуальная модель информационной безопасности. 10](#_Toc472106067)

[1.3. Угрозы конфиденциальной информации 13](#_Toc472106068)

[1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией. 15](#_Toc472106069)

[1. Область применения Государственный стандарт РФ ГОСТ Р 50922 - 96 20](#_Toc472106070)

[2. Общие положения 21](#_Toc472106071)

[3 Стандартизованные термины и их определения 21](#_Toc472106072)

[3.1 Основные понятия 21](#_Toc472106073)

[3.2 Организация защиты информации 21](#_Toc472106074)

[4. Приложение А (справочное) 21](#_Toc472106075)

[1 ОБЛАСТЬ ПРИМЕНЕНИЯ 21](#_Toc472106076)

[2 ОБЩИЕ ПОЛОЖЕНИЯ 21](#_Toc472106077)

[3 СТАНДАРТИЗОВАННЫЕ ТЕРМИНЫ И ИХ ОПРЕДЕЛЕНИЯ 22](#_Toc472106078)

[3.1 Основные понятия 22](#_Toc472106079)

[3.2 Организация защиты информации 24](#_Toc472106080)

[ГОСТ Р 50922-96 Приложение А (справочное) Термины и определения, необходимые для понимания текста стандарта 26](#_Toc472106081)

[Способы защиты информации 27](#_Toc472106082)

[3.1. Общие положения 28](#_Toc472106083)

[3.2. Характеристика защитных действий 35](#_Toc472106084)

# Введение

Примечательная особенность нынешнего периода - переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергические ресурсы. Ресурсами, как известно, называют элементы экономического потенциала, которыми располагает общество и которое при необходимости могут быть использованы для достижения конкретной цели хозяйственной деятельности. Давно стали привычными и общеупотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Но вот появилось понятие "информационные ресурсы", и хотя оно узаконено, но осознано пока еще недостаточно. Информационные ресурсы - отдельные документы и отдельные массивы, документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить. Собственная информация для производителя представляет значительную ценность, так как нередко получение (создание) такой информации - весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами.

Особое место отводится информационным ресурсам в условиях рыночной экономики.

Важнейшим фактором рыночной экономики выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее (ВРЕМЯ-ДЕНЬГИ!!!) производит и продает. В сущности это универсальное правило рынка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47% охраняемых сведений добывается с помощью технических средств промышленного шпионажа.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Как видно из этого определения целей защиты, информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

Основное внимание уделяется защите конфиденциальной информации, с которой большей частью встречаются предприниматели негосударственного сектора экономики.

Люди осознают и отдают себе отчет в сложности проблемы защиты информации вообще, и с помощью технических средств в частности. Тем не менее взгляд на эту проблему излагается на этом Web-сайте, считается, что этим охватывается не все аспекты сложной проблемы, а лишь определенные ее части.

# Концепция информационной безопасности

## 1. Основные концептуальные положения системы защиты информации

## 2. Концептуальная модель информационной безопасности

## 3. Угрозы конфиденциальной информации

## 4. Действия, приводящие к неправомерному овладению конфиденциальной информацией

"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств" (Закон РФ "Об участии в международном информационном обмене").

Постулаты

Информация - это всеобщее свойство материи.

Любое взаимодействие в природе и обществе основано на информации.

Всякий процесс совершения работы есть процесс информационного взаимодействия.

Информация - продукт отражения действительности.

Действительность отражается в пространстве и времени.

Ничего не происходит из ничего.

Информация сохраняет значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации - ПАМЯТЬ.

Ничто не исчезает просто так.

Понятие "информация" сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается, каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики ИНФОРМАЦИИ - информационным веком.

Правомерно задать вопрос: что же такое информация? В литературе дается такое определение: информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Известно, что информация может иметь различную форму, включая данные, заложенные в компьютерах, "синьки", кальки, письма или памятные записки, досье, формулы, чертежи, диаграммы, модели продукции и прототипы, диссертации, судебные документы и др.

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства, и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности - такие, как персонал, материальные и финансовые средства и информацию.

# 1.1 Основные концептуальные положения системы защиты информации.

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;

значительное число фирм, специализирующихся на решении вопросов защиты информации;

достаточно четко очерченная система взглядов на эту проблему;

наличие значительного практического опыта и др.

И, тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт также показывает, что:

обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;

безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;

никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту.

С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

Непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;

Плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

Целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;

Конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;

Активной. Защищать информацию необходимо с достаточной степенью настойчивости;

Надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;

Универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;

Комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства.

Комплексный характер защиты проистекает из того, что защита - это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденций.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным условиям:

охватывать весь технологический комплекс информационной деятельности;

быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;

быть открытой для изменения и дополнения мер обеспечения безопасности информации;

быть нестандартной, разнообразной. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;

быть простой для технического обслуживания и удобной для эксплуатации пользователями;

быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;

быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы. К системе безопасности информации предъявляются также определенные требования:

четкость определения полномочии и прав пользователей на доступ к определенным видам информации;

предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

сведение к минимуму числа общих для нескольких пользователей средств защиты;

учет случаев и попыток несанкционированного доступа к конфиденциальной информации;

обеспечение оценки степени конфиденциальной информации;

обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя. Система защиты информации как любая система должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий;

организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами - такими, как служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и др.;

аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно СЗИ;

информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;

математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности. Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

# 1.2. Концептуальная модель информационной безопасности.

Понимая информационную безопасность как "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций", правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать методы моделирования, при которых формируется как бы "заместитель" реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить следующие компоненты модели информационной безопасности на первом уровне декомпозиции.

По нашему мнению, такими компонентами концептуальной модели безопасности информации могут быть следующие:

объекты угроз;

угрозы;

источники угроз;

цели угроз со стороны злоумышленников;

источники информации;

способы неправомерного овладения конфиденциальной информацией (способы доступа);

направления защиты информации;

способы защиты информации;

средства защиты информации.

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, кон-фиденциальности, полноты и доступности. Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.



Рисунок 2.1 – Логическая цепочка угроз и их проявлений

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства. Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программ-но, так и смешанно-программно-аппаратными средствами.

В качестве способов защиты выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу. В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме.

Основные элементы концептуальной модели будут рассмотрены более подробно в следующих разделах книги. Концепция безопасности является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз.



# 1.3. Угрозы конфиденциальной информации

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями. Такими действиями являются:

ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;

модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;

разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечет за собой определенный ущерб - моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале - полностью, реально - значительно или хотя бы частично. Но и это удается далеко не всегда.

С учетом этого угрозы могут быть классифицированы по следующим кластерам :

по величине принесенного ущерба:

предельный, после которого фирма может стать банкротом;

значительный, но не приводящий к банкротству;

незначительный, который фирма за какое-то время может компенсировать и др.;

по вероятности возникновения:

весьма вероятная угроза;

вероятная угроза;

маловероятная угроза;

по причинам появления:

стихийные бедствия;

преднамеренные действия;

по характеру нанесенного ущерба:

материальный;

моральный;

по характеру воздействия:

активные;

пассивные;

по отношению к объекту:

внутренние;

внешние.

Источниками внешних угроз являются:

недобросовестные конкуренты;

преступные группировки и формирования;

отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

администрация предприятия;

персонал;

технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;

17% угроз совершается извне - внешние угрозы;

1% угроз совершается случайными лицами.

Угроза - это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.



Рисунок 2.2 – Угрозы информационной безопасности

# 1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;

источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;

промежуточная ситуация - это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

В общем, факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации .

Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение (встречи, переписка и др.); выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов. Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видео мониторинг).

Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электро-магнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении "продать" секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами. Если исходить из комплексного подхода к обеспечению инфор-мационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников. Такой подход к классификации действий, способствующих неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной безопасности.

С учетом изложенного остается рассмотреть вопрос, какие условия способствуют неправомерному овладению конфиденциальной ин-формацией. Указываются следующие условия:

разглашение (излишняя болтливость сотрудников) - 32%;

несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок - 24%;

отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности - 14%;

традиционный обмен производственным опытом - 12%;

бесконтрольное использование информационных систем - 10%;

наличие предпосылок возникновения среди сотрудников конфликтных ситуаций 8%;

а также отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа кадров по сплочению коллектива.

Среди форм и методов недобросовестной конкуренции находят наибольшее распространение:

экономическое подавление, выражающееся в срыве сделок и иных соглашений (48%),

парализации деятельности фирмы (31%),

компрометации фирмы (11%),

шантаже руководителей фирмы (10%);

физическое подавление:

ограбления и разбойные нападения на офисы, склады, грузы (73%),

угрозы физической расправы над руководителями фирмы и ведущими специалистами (22%),

убийства и захват заложников (5%);

информационное воздействие:

подкуп сотрудников (43%),

копирование информации (24%),

проникновение в базы данных (18%),

продажа конфиденциальных документов (10%),

подслушивание телефонных переговоров и переговоров в помещениях (5%),

а также ограничение доступа к информации, дезинформация;

финансовое подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество; психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.

Основными угрозами информации являются ее разглашение, утечка и несанкционированный доступ к ее источникам. Каждому из условий неправомерного овладения конфиденциальной информацией можно поставить в соответствие определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия. Совокупность определений, каналов, способов и средств представляется в виде следующей схемы.

Рисунок 2.3 – Модель реализации угроз информационные безопасности

# 1. Область применения Государственный стандарт РФ ГОСТ Р 50922 - 96

ГОСТ Р 50922 - 96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

Основные термины и определения

Дата введения 1.07.97 г.

# 2. Общие положения

# 3 Стандартизованные термины и их определения

# 3.1 Основные понятия

# 3.2 Организация защиты информации

# 4. Приложение А (справочное)

## 1 ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт устанавливает основные термины и их определения в области защиты информации.

Термины, установленные настоящим стандартом, обязательны для применения во всех видах документации и литературы по защите информации.

Настоящий стандарт применяется совместно с ГОСТ РВ 50170-92.

## 2 ОБЩИЕ ПОЛОЖЕНИЯ

Установленные в стандарте термины расположены в систематизированном порядке, отражающем систему понятий в данной области знания.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два (три, четыре и т.п.) термина, имеющие общие терминоэлементы.

Разрешается, при необходимости, уточнять приведенные определения, вводя дополнительные признаки, раскрывающие значения терминов, без искажения смысла определения.

Термины и определения общетехнических понятий, необходимые для понимания текста стандарта, приведены в приложении А.

## 3 СТАНДАРТИЗОВАННЫЕ ТЕРМИНЫ И ИХ ОПРЕДЕЛЕНИЯ

### 3.1 Основные понятия

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание: Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации - защита информации: Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от утечки - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

Защита информации от несанкционированного воздействия - защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Зашита информации от непреднамеренного воздействия - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа - защита информации от НСД: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Примечание: Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации от [иностранной] разведки - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой.

Защита информации от [иностранной] технической разведки - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

Защита информации от агентурной разведки - деятельность по предотвращению получения защищаемой информации агентурной разведкой.

Цель защиты информации - желаемый результат защиты информации.

Примечание: Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации - степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности зашиты информации - мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации - значения показателей эффективности защиты информации, установленные нормативными документами.



Рисунок 4.1 – Угрозы безопасности информационных систем

### 3.2 Организация защиты информации

Организация защиты информации - содержание и порядок действий по обеспечению защиты информации.

Система защиты информации - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Мероприятие по защите информации - совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации- совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

Техника защиты информации - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Способ защиты информации - порядок и правила применения определенных принципов и средств защиты информации.

Категорирование защищаемой информации [объекта защиты] - установление градаций важности защиты защищаемой информации [объекта защиты].

Метод [способ] контроля эффективности защиты информации - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Контроль состояния защиты информации - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Средство защиты информации - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Контроль организации защиты информации - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Организационный контроль эффективности зашиты информации- проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности зашиты информации - контроль эффективности защиты информации, проводимой с использованием средств контроля.

## ГОСТ Р 50922-96 Приложение А (справочное) Термины и определения, необходимые для понимания текста стандарта

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Доступ к информации - получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Субъект доступа к информации - субъект доступа: участник правоотношений в информационных процессах.

Примечание: Информационные процессы - процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

Носитель информации - физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Собственник информации - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Пользователь [потребитель] информации - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

Право доступа к информации - право доступа: совокупность правил доступа к информации, установленных правовыми документами или собственником, владельцем информации.

Правило доступа к информации - правило доступа: совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Орган защиты информации - административный орган, осуществляющий организацию защиты информации.

# Способы защиты информации

3.1. Общие положения

3.2. Характеристика защитных действий

Способы - это порядок и приемы использования сил и средств для достижения поставленной цели по защите конфиденциальной информации.

1. Подальше положишь - поближе возьмешь.

2. Береженого Бог бережет.

3. На Бога надейся, а сам не плошай.

4. Сначала подумай, потом говори.

5. Не зная броду, не суйся в воду.

6. Семь раз отмерь, один раз отрежь.

7. Дело мастера боится.

8. Негоже, когда сапоги тачает пирожник, а пироги печет сапожник.

9. Отыщи всему начало, и ты многое поймешь (К. Прутков).

Любое действие человека, ориентированное на достижение каких-либо результатов, реализуется определенными способами. Естественно, что имеющийся опыт по защите информации достаточно четко определил совокупность приемов, сил и средств, ориентированных на обеспечение информационной безопасности. С учетом этого можно так определить понятие способов защиты информации: способы защиты информации - это совокупность приемов, сил и средств, обеспечивающих конфиденциальность, целостность, полноту и доступность информации, и противодействие внутренним и внешним угрозам.

Естественно предположить, что каждому виду угроз присущи свои специфические способы, силы и средства.

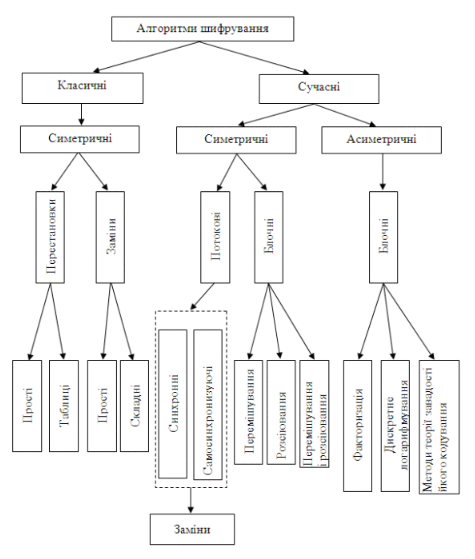


Рисунок 5.1 – Классификация алгоритмов шифрования

## 3.1. Общие положения

Обеспечение информационной безопасности достигается системой мер, направленных:

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. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;

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

на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения (если хотите - и добывания) информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции. Особое внимание в этом виде деятельности должно отводиться изучению собственных сотрудников. Среди них могут быть и недовольные, и неопытные, и "внедренные".

Обнаружение угроз - это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов. В числе мероприятий по обнаружению угроз значительную роль могут сыграть не только сотрудники СБ, но и сотрудники линейных подразделений и служб фирмы, а также технические средства наблюдения и обнаружения правонарушений.

Пресечение или локализация угроз - это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

предотвращение разглашения и утечки конфиденциальной информации;

воспрещение несанкционированного доступа к источникам конфиденциальной информации; сохранение целостности, полноты и доступности информации;

соблюдение конфиденциальности информации;

обеспечение авторских прав.

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих коммерческую тайну предприятия. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять коммерческую тайну. Одним из важных мероприятий является система контроля за сохранностью коммерческих секретов.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной "информации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации и реализацией организационных, организационно-технических и технических мероприятий по противодействию НСД.

На практике в определенной степени все мероприятия по использованию технических средств защиты информации подразделяются на три группы:

организационные (в части технических средств);

организационно-технические;

технические.

Организационные мероприятия - это мероприятия ограничительного характера, сводящиеся основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

определение границ охраняемой зоны (территории);

определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;

определение "опасных", с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений;

выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;

реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации. В этих целях возможно использование:

технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радио- и часофикации и др.;

технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и др.

Энергетические - это снижение интенсивности излучения и работа РЭС на пониженных мощностях.

Технические мероприятия - это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.

Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.

Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.

Подавление - это создание активных помех средствам злоумышленников.

Дезинформация - это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания.

Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаются в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления.

## 3.2. Характеристика защитных действий

Защитные действия ориентированы на пресечение разглашения, защиту информации от утечки и противодействия несанкционированному доступу.

Защитные действия, способы и мероприятия по обеспечению информационной безопасности можно классифицировать по основным характеристикам и объектам защиты по таким параметрам, например, как ориентация, характер угроз, направления, способы действий, охват, масштаб и др.

Защитные действия по ориентации можно классифицировать как действия, направленные на защиту персонала, материальных и финансовых средств и информации как ресурса.

По направлениям - это правовая, организационная и инженерно-техническая защита.

По способам - это предупреждение, выявление, обнаружение, пресечение и восстановление.

По охвату защитные меры могут быть ориентированы на защиту территории фирмы, зданий, отдельных (выделенных) помещений, конкретных видов аппаратуры или технических средств и систем или отдельных элементов зданий, помещений, аппаратуры, опасных с точки зрения несанкционированного доступа к ним или оборудования каналов утечки информации.

Применение защитных мер можно рассматривать и в пространственном плане. Так, например, известно, что распространение (разглашение, утечка или НСД) осуществляется от источника информации через среду к злоумышленнику.

Источником информации могут быть люди, документы, технические средства, отходы и др. Носителем информации может быть либо поле (электромагнитное, акустическое), либо вещество (бумага, материал, изделие и т.д.). Средой является воздушное пространство, жесткие среды (стены, коммуникации).

Злоумышленник обладает необходимыми средствами приема акустической и электромагнитной энергии, средствами воздушного наблюдения и возможностью обрабатывать материально-вещественные формы представления информации.

Чтобы исключить неправомерное овладение конфиденциальной информацией, следует локализовать (выключить, ослабить сигнал, зашифровать и др.) источник информации.

С увеличением масштабов распространения и использования ПЭВМ и информационных сетей усиливается роль различных факторов, вызывающих утечку, разглашение и несанкционированный доступ к информации. К ним относятся:

несанкционированные и злоумышленные действия персонала и пользователя;

ошибки пользователей и персонала;

отказы аппаратуры и сбои в программах;

стихийные бедствия, аварии различного рода и опасности.

В соответствии с этими основными целями защиты информации в ПЭВМ и информационных сетях являются:

обеспечение юридических норм и прав пользователей в отношении ДОСТУПА к информационным и другим сетевым ресурсам, предусматривающее административный надзор за информационной деятельностью, включая меры четкой персональной ответственности за соблюдение правил пользования и режимов работы;

предотвращение потерь и утечки информации, перехвата и вмешательства на всех уровнях, для всех территориально разделенных объектов;

обеспечение целостности данных на всех этапах и фазах их преобразования и сохранности средств программного обеспечения.

В связи с тем, что информационная сеть, в отличие от автономной ПЭВМ, является территориально распределенной системой, она требует принятия специальных мер и средств защиты. Средства защиты должны предотвращать:

определение содержания передаваемых сообщений;

внесение изменений в сообщения;

необоснованный отказ в доступе;

несанкционированный доступ;

ложную инициализацию обмена;

возможность измерения и анализа энергетических и других характеристик информационной системы.

Если это нецелесообразно или невозможно, то нарушить информационный контакт можно за счет использования среды распространения информации. Например, при почтовой связи использовать надежного связного и доставить почтовое отправление абоненту, полностью исключив возможность несанкционированного доступа к нему со стороны. Или исключить возможность подслушивания путем использования специального помещения, надежно защищенного о; такого вида НСД. И, наконец, можно воздействовать на злоумышленника или на его средства путем постановки активных средств воздействия (помехи).

В каждом конкретном случае реализации информационного контакта используются и свои специфические способы воздействия как на источник, так и на среду и на злоумышленника. В качестве примера рассмотрим матрицу, характеризующую взаимосвязь целей защиты информации и механизмов ее защиты в процессе телекоммуникационного обмена в распределенных автоматизированных системах. Одновременно на ней отражены и защитные возможности тех или иных механизмов.

Заключение

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб.

Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.

В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации.

Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др.

Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности,

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.

Основными целями защиты информации являются обеспечение конфиденциальности, целостности, полноты и достаточности информационных ресурсов.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

Совокупность способов обеспечения информационной безопасности может быть подразделена на общие и частные, применение которых обусловливается масштабностью защитных действий.

# Приложение Б

# Алгоритм шифрования DES

Рассмотрим пример кода симметричного шифрования DES:

**package** Source;

**import** javax.crypto.\*;

**import** java.io.IOException;

**import** java.io.UnsupportedEncodingException;

**import** java.security.InvalidKeyException;

**import** java.security.Key;

**import** java.security.NoSuchAlgorithmException;

**public class** cipherTest

{

*//Здесь мы создаем два объекта — один для шифрования, другой — дешифрования.*

Cipher **ecipher**;

Cipher **dcipher**

**public static void** main(String[] args) **throws** java.security.InvalidKeyException, IOException, IllegalBlockSizeException, BadPaddingException, NoSuchAlgorithmException, NoSuchPaddingException {

*//в этих двух cтрочках мы задаем параметры для объектов и передаем туда ключ.*

*//Ключ генерируется такой конструкцией:*

SecretKey key = **null**;

key = KeyGenerator.*getInstance*(**"DES"**).generateKey();

cipherTest encrypter = **new** cipherTest(key);

String OStr1=**"simple string"**;

String SStr = encrypter.encrypt(OStr1);

String OStr2 = encrypter.decrypt(SStr);

System.***out***.println(**"Open String: "**+OStr1+

**"\nAfter encripting: "**+SStr+**"\nAfter decripting: "**+OStr2);

}

**public** cipherTest(SecretKey key) **throws** NoSuchAlgorithmException, NoSuchPaddingException, InvalidKeyException

{

**ecipher** = Cipher.*getInstance*(**"DES"**);

**dcipher** = Cipher.*getInstance*(**"DES"**);

**ecipher**.init(Cipher.***ENCRYPT\_MODE***, key);

**dcipher**.init(Cipher.***DECRYPT\_MODE***,key);

}

*//Мы задаем, какой алгоритм будем использовать для шифрования и генерируем*

*//ключ.*

*//Рассмотрим функцию шифрования:*

**private** String encrypt(String str) **throws** UnsupportedEncodingException,

IllegalBlockSizeException, BadPaddingException {

**byte**[] utf8 = str.getBytes(**"UTF8"**);

**byte**[] enc = **ecipher**.doFinal(utf8);

**return new** sun.misc.BASE64Encoder().encode(enc);

}

*//В функцию передается строка для шифрования. Но, функции шифрования работают*

*//с битовыми массивами, поэтому строку переводим в битовый массив. Также, при*

*//создании строки играет роль кодировка. Чтобы избежать неприятностей, нужно*

*//использовать Base64-кодирование.*

*//Функция дешифрования:*

**private** String decrypt(String str) **throws** IOException, IllegalBlockSizeException,

BadPaddingException {

**byte**[] dec = **new** sun.misc.BASE64Decoder().decodeBuffer(str);

**byte**[] utf8 = **dcipher**.doFinal(dec);

**return new** String(utf8, **"UTF8"**);

}

*//Здесь мы принимаем уже зашифрованную строку, которую побитово*

*//расшифровываем*

}