Министерство образования и науки Российской Федерации

Федеральное бюджетное образовательное учреждение

высшего профессионального образования

Уфимский Государственный Технический Университет

ВTиЗИ

Лабораторная работа №2

Комбинаторно-морфологический метод синтеза рациональных

наборов средств защиты для систем защиты информации

дисциплина: «Управление информационной безопасностью»

Выполнили ст. гр.БПС-403

Ганцев С. В.

Захаров Д. Ю.

Проверила: д.т.н. Машкина И.В.

Уфа 2015

# Комбинаторно-морфологический метод синтеза рациональных наборов средств защиты для систем защиты информации.

**Цель работы:** осуществить синтез системы обеспечения информационной безопасности на основе выбора рациональных наборов средств защиты периметра и хоста, входящих в Государственный реестр сертифицированных средств защиты с учетом выделенных ресурсов (денежных средств) на основе комбинаторно-морфологического метода синтеза рациональных наборов средств защиты для систем обеспечения информационной безопасности.

**Ход работы:**

1. В ходе лабораторной работы были разработали варианты синтезируемого набора средств защиты для нескольких систем:

* Система шифрования при хранении
* Система резервного копирования
* Система контроля целостности
* Система разграничения доступа

Таблица 1. Выбор альтернатив сертифицированных средств защиты

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Система шифрования при хранении | TrueCrypt | Folder Lock | PGP Desktop | CyberSafe Top Secret | - |
| Система резервного копирования | Exiland Backup Professional | Acronis  Backup | Clonezilla | Norton ghost | Handy  Backup |
| Система контроля целостности | ПКЦ | ФИКС-UNIX 1.0 | integrity | ФИКС-DOS 1.0 | Check |
| Система разграничения доступа | Secret net | Криптон-щит | Dallas lock | Аккорд | Аура |

2. Далее был осуществлен выбор критериев оценки элементарных альтернатив: показатели «защищенности» и показатели «издержек» для системы шифровании при хранении.

Показатели защищенности для системы шифрования при хранении:

* Поддержка ЭЦП
* Шифрование системного диска
* Двухфакторная аутентификация
* Скорость чтения
* Поддержка токенов

Показатели издержек для системы шифрования при хранении:

* Цена
* Минимальный объем ОЗУ

Таблица 2. Выбор параметров для системы шифрования при хранении

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | ЭЦП | Шифр. системного диска | Двухф. аут. | Скорость чтения (Мб/с) | Поддержка токенов. | Количество ОЗУ  (Мб) | Цена  (Руб.) |
| TrueCrypt | Нет | Да | Нет | 250 | Да | 1024 | беспл. |
| Folder Lock | Нет | Нет | Нет | 47 | Нет | 2048 | 2600 |
| PGP Desktop | Да | Да | Нет | 35 | Нет | 4096 | 13000 |
| CyberSafe Top Secret | Да | Нет | Да | 62 | Да | 2048 | 3250 |

Далее значения показателей "защищенность" и "издержки" были переведены в относительные единицы.

Таблица 3. Критерии для системы шифрования при хранении в относительных единицах

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | ЭЦП | Шифр. системного диска | Двухф. аут. | Скорость чтения | Поддержка токенов. | Количество ОЗУ | Цена |
| TrueCrypt | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| Folder Lock | 0 | 0 | 0 | 0,558 | 0 | 0,33 | 0,2 |
| PGP Desktop | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| CyberSafe Top Secret | 1 | 0 | 1 | 0,125 | 1 | 0,33 | 0,25 |

3. Далее был осуществлен выбор критериев оценки элементарных альтернатив: показатели «защищенности» и показатели «издержек» для системы резервного копирования.

Показатели защищенности для системы резервного копирования:

* Наличие функции резервирования по расписанию
* Наличие функции восстановления отдельных файлов и томов
* Наличие дублирования (резервирование на несколько источников)
* Шифрование при резервировании

Показатели издержек для системы резервного копирования:

* Цена
* Минимальный объем ОЗУ

Таблица 4. Выбор параметров для системы резервного копирования.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | Резерв. по распис. | Восст. томов и файлов | Ф-я  дубл-я | Шифр. при резерв. | Объем ОЗУ (Мб) | Цена  (руб.) |
| Exiland Backup Professional | Да | Нет | Да | Нет | 1024 | 2950 |
| Acronis | Да | Да | Да | Да | 2048 | 16990 |
| Clonezilla | Нет | Нет | Да | Да | 196 | бесп. |
| Norton ghost | Да | частично | Да | Да | 1024 | 1749 |
| HandyBackUp | Да | частично | Нет | Да | 1024 | 2900 |

Далее значения показателей "защищенность" и "издержки" были переведены в относительные единицы.

Таблица 5. Параметры для систем резервного копирования, выраженные в относительных единицах

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | Резерв. по распис. | Восст. томов и файлов | Ф-я  дубл-я | Шифр. при резерв. | Объем ОЗУ | Цена |
| Exiland Backup Professional | 1 | 0 | 1 | 0 | 0.447 | 0.173 |
| Acronis | 1 | 1 | 1 | 1 | 1 | 1 |
| Clonezilla | 0 | 0 | 1 | 1 | 0 | 0 |
| Norton ghost | 1 | 0,5 | 1 | 1 | 0.447 | 0.102 |
| HandyBackUp | 1 | 0,5 | 0 | 1 | 0.447 | 0.17 |

4. Далее был осуществлен выбор критериев оценки элементарных альтернатив: показатели «защищенности» и показатели «издержек» для системы контроля целостности.

Показатели защищенности для системы контроля целостности:

* Используемый метод контроля
* Возможность хранение хэшей на съемных носителях
* Возможность контроля определенного списка файлов

Показатели издержек для систем контроля целостности:

* Цена
* Минимальный объем ОЗУ

Таблица 6. Выбор параметров для системы контроля целостности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Параметры  Средство | Метод контроля | Хранение хэша на съем. носит. | Контроль списка файлов | Цена.  (руб.) | Объем ОЗУ (Мб) |
| ПКЦ | Хэш | Да | Да | 1050 | 256 |
| ФИКС-UNIX 1.0 | Хэш | Нет | Да | 2080 | 128 |
| integrity | Хэш | Нет | Нет | 33000 | 128 |
| ФИКС 2.0.1 | Хэш + ЭЦП | Нет | Да | 2900 | 256 |
| Check | Хэш + ЭЦП | Да | Да | 2600 | 1024 |

Далее значения показателей "защищенность" и "издержки" были переведены в относительные единицы.

Таблица 7. Параметры для систем контроля целостности, выраженные в относительных единицах

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Параметры  Средство | Метод контроля | Хранение хэша на съем. носит. | Контроль списка файлов | Цена. | Объем ОЗУ |
| ПКЦ | 0 | 1 | 1 | 0 | 0.142 |
| ФИКС-UNIX 1.0 | 0 | 0 | 1 | 0,457 | 0 |
| integrity | 0 | 0 | 0 | 1 | 0 |
| ФИКС 2.0.1 | 1 | 0 | 1 | 0,822 | 0.142 |
| Check | 1 | 1 | 1 | 0,688 | 1 |

5. Далее был осуществлен выбор критериев оценки элементарных альтернатив: показатели «защищенности» и показатели «издержек» для системы разграничения доступа.

Показатели защищенности для системы разграничения доступа:

* Наличие функции автоматической блокировки доступа к ресурсам во время отсутствия пользователя
* Возможность контроля доступа доступа на уровне процессов ОС
* Функция дополнительной аутентификации при выходе из сеанса
* Механизмы логирования

Показатели издержек для систем контроля целостности:

* Цена
* Минимальный объем ОЗУ

Таблица 8. Выбор параметров для системы разграничения доступа

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | авто. блокир. доступа | контроль доступа на уровне ОС | Ф-я  доп. аутентиф | механизмы логирования | Объем ОЗУ (Мб) | Цена  (руб.) |
| Secret net | да | да | да | Нет | 2048 | 7700 |
| Криптон-щит | да | да | да | Да | 1024 | 4800 |
| Dallas lock | да | да | да | Да | 1024 | 10000 |
| Аккорд | нет | нет | нет | Да | 512 | 11000 |
| Аура | да | да | нет | Да | 256 | 6000 |

Далее значения показателей "защищенность" и "издержки" были переведены в относительные единицы.

Таблица 9. Параметры для систем контроля целостности, выраженные в относительных единицах

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Параметры  Средство | авто. блокир. доступа | контроль доступа на уровне ОС | Ф-я  доп. аутентиф | механизмы логирования | Объем ОЗУ | Цена |
| Secret net | 1 | 1 | 1 | 0 | 1 | 0.467 |
| Криптон-щит | 1 | 1 | 1 | 1 | 0.428 | 0 |
| Dallas lock | 1 | 1 | 1 | 1 | 0.428 | 0.838 |
| Аккорд | 0 | 0 | 0 | 1 | 0.142 | 1 |
| Аура | 1 | 1 | 0 | 1 | 0 | 0.193 |

6. Далее были подсчитаны значения показателей защищенности и издержек для каждой системы.

Таблица 10. Значения показателей "защищенность" и "издержки" для каждой системы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Функциональная подсистема | Отношение показателей "защищенность" к "издержкам" | | | | |
| *1* | *2* | *3* | *4* | *5* |
| Система шифрования при хранении | 3  0 | 0,0058  0,5333 | 2  2 | 3,1255  0,5833 |  |
| Система резервного копирования | 2  0,62 | 4  2 | 2  0 | 3,5  0,55 | 2,5  0,6177 |
| Система контроля целостности | 2  0,1428 | 1  0,4577 | 0  1 | 2  0,965 | 3  1,6888 |
| Система разграничения доступа | 3  1,4677 | 4  0,4285 | 4  1,2672 | 1  1,1428 | 3  1,1935 |

7. Далее были выбраны наилучшие варианты набора средств защиты:

Таблица 11. Наилучшие варианты набора средств защиты

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Места  набора  средств  защиты | Значение целевой функции | Функциональные подсистемы | | | |
| Система шифр. при хранении | Система резервного копирования | Система контроля целостности | Система разграничения доступа |
| 1 | 29.726 | TrueCrypt | Clonezilla | ПКЦ | Аура |
| 2 | 19,25 | TrueCrypt | Clonezilla | ПКЦ | Криптон-щит |
| 3 | 13.817 | TrueCrypt | Clonezilla | ФИКС-UNIX 1.0 | Аура |
| 4 | 12.973 | TrueCrypt | Norton ghost | ПКЦ | Аура |
| 5 | 11.282 | TrueCrypt | Clonezilla | ФИКС-UNIX 1.0 | Криптон-щит |

**Листинг программного кода:**

# подключаем модуль для работы с файлом конфигурации

require 'yaml'

# Путь к файлу конфигурации

PATH = 'config2.yml

# Грузим данные из файла конфигурации

config = YAML::load(open(PATH))

$general = []

config.each\_key do |set\_name|

# Для удобства определяем набор средств защиты

current\_set = config[set\_name]

# # Определяем названия критериев и издержек

# criteria = current\_set['criteria']

# costs = current\_set['costs']

# Для удобства определяем альтернативы конкретного набора

alternatives = current\_set['alternatives']

# Определяем первую альтернативу в наборе для использования в качестве эталона

first\_alternative = alternatives.first[1]

# Объявляем массивы минимальных и максимальных критериев и издержек

max\_criteria = first\_alternative['criteria'].clone

min\_criteria = first\_alternative['criteria'].clone

max\_costs = first\_alternative['costs'].clone

min\_costs = first\_alternative['costs'].clone

# Пройдемся по каждому элементу набора для определения массивов минимальных

# и максимальных критериев и издержек

alternatives.each\_key do |alternative\_name|

# Для удобства определяем конкретную альтернативу

alternative = current\_set['alternatives'][alternative\_name]

# Для удобства определяем критерии альтернативы

alternative\_criteria = alternative['criteria']

# Пройдемся по каждому из критериев альтернативы для нахождения

# наименьшего и наибольшего значений

alternative\_criteria.each\_index do |criteria\_index|

if alternative\_criteria[criteria\_index] > max\_criteria[criteria\_index]

max\_criteria[criteria\_index] = alternative\_criteria[criteria\_index]

elsif alternative\_criteria[criteria\_index] < min\_criteria[criteria\_index]

min\_criteria[criteria\_index] = alternative\_criteria[criteria\_index]

end

end

# Для удобства определяем издержки альтернативы

alternative\_costs = alternative['costs']

# Пройдемся по каждому из издержек альтернативы для нахождения

# наименьшего и наибольшего значений

alternative\_costs.each\_index do |costs\_index|

if alternative\_costs[costs\_index] > max\_costs[costs\_index]

max\_costs[costs\_index] = alternative\_costs[costs\_index]

elsif alternative\_costs[costs\_index] < min\_costs[costs\_index]

min\_costs[costs\_index] = alternative\_costs[costs\_index]

end

end

end

set\_array = []

# Пройдемся ещё раз по каждому элементу набора для определения критетиев и издержек

alternatives.each\_key do |alternative\_name|

# Для удобства определяем конкретную альтернативу

alternative = current\_set['alternatives'][alternative\_name]

alternative['sum\_criteria'] = 0

# Для удобства определяем критерии альтернативы

alternative\_criteria = alternative['criteria']

# Пройдемся по каждому из критериев альтернативы для определения нового значения

alternative\_criteria.each\_index do |criteria\_index|

min = min\_criteria[criteria\_index]

max = max\_criteria[criteria\_index]

if min != max

alternative\_criteria[criteria\_index] =

( alternative\_criteria[criteria\_index] - min ).to\_f / ( max - min )

alternative['sum\_criteria'] += alternative\_criteria[criteria\_index]

else

alternative\_criteria[criteria\_index] = 0

end

end

alternative['sum\_costs'] = 0

# Для удобства определяем критерии альтернативы

alternative\_costs = alternative['costs']

# Пройдемся по каждому из критериев альтернативы для определения нового значения

alternative\_costs.each\_index do |costs\_index|

# current\_costs = alternative\_costs[costs\_index]

min = min\_costs[costs\_index]

max = max\_costs[costs\_index]

if min != max

alternative\_costs[costs\_index] =

( alternative\_costs[costs\_index] - min ).to\_f / ( max - min )

alternative['sum\_costs'] += alternative\_costs[costs\_index]

else

alternative\_costs[costs\_index] = 0

end

end

alternative['name'] = alternative\_name

set\_array << alternative

end

$general << set\_array

end

puts $general

# Массив конечных данных

$result = []

# Номер текущего наборы - текущий уровень

$combination = []

def branch (set\_number)

if set\_number == $general.length

w1 = 0

w2 = 0

combination\_name = ''

$combination.each\_index do |index|

w1 += $combination[index]['sum\_criteria']

w2 += $combination[index]['sum\_costs']

combination\_name += $combination[index]['name']

end

combination\_object = {

value: w1.to\_f / w2,

name: combination\_name

}

$result << combination\_object

$combination.pop

else

$general[set\_number].each\_index do |index|

$combination[set\_number] = $general[set\_number][index]

branch (set\_number + 1)

end

end

end

branch 0

$result = $result.sort\_by { |hsh| hsh[:value] }

puts $result

**Вывод**: В процессе выполнения лабораторной работы был осуществили выбор наилучшего набора средства защиты на основе комбинаторно-морфологического метода. Таким образом наибольший показатель защищенности оказался у следующего набора:

* Система шифрования при хранении – TrueCrypt
* Система резервного копирования - Clonezilla
* Система контроля целостности – ПКЦ
* Система разграничения доступа - Аура

**СПИСОК ЛИТЕРАТУРЫ**

1. Блог компании «КИБЕРСОФТ» - *Сравнение настольных программ для шифрования* [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/company/cybersafe/blog/252561/, свободный.

1. Блог компании «Veeam Software» - *Резервное копирование физических машин* [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/company/veeam/blog/261481/, свободный.

1. *Резервное копирование файлов. Exiland Backup* [Электронный ресурс]. – Режим доступа: http://www.exiland-backup.com/ru/, свободный.

1. *Choose your backup* [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/489>, свободный.

1. *Minimum System Requirements for Clonezilla live* [Электронный ресурс]. – Режим доступа: http://www.clonezilla.org/, свободный.

1. *Государственный* реестр сертефицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/489>, свободный.

1. *Государственный* реестр сертефицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/489>, свободный.

1. *Государственный* реестр сертефицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/489>, свободный.

1. *Государственный* реестр сертефицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – Режим доступа: <http://fstec.ru/component/attachments/download/489>, свободный.

2. *Программа «ПКЦ»* – Режим доступа: http://www.agat.by/products/security-soft/complex-integrity-control-soft/, свободный.

2. *Средство фиксации и контроля целостности информации "ФИКС-Unix 1.0"*– Режим доступа: http://www.cbi-info.ru/groups/page-347.htm, свободный.

2. *Средство контроля целостности СКЗИ и СФК integrity. Руководство оператора* – Режим доступа: http://www.cryptocom.ru/docs/cryptopack21-integrity.pdf, свободный.

2. *Средство фиксации и контроля исходного состояния программного комплекса "ФИКС" (версия 2.0.1)* – Режим доступа: http://www.cbi-info.ru/groups/page-345.htm, свободный.

2. *Программы контроля "Check" для сертифицированных версий продуктов Microsoft* – Режим доступа: http://www.altx-soft.ru/groups/page-267.htm, свободный.

3. *Система разграничения доступа «КРИПТОН-ЩИТ»*  [Электронный ресурс]. – Режим доступа: http://ancud.ru/srd.html, свободный.

4. *СЗИ от НСД Secret Net* [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/products/secret\_net/, свободный.

4. *Dallas Lock – сертифицированная система защиты информации от несанкционированного доступа.* [Электронный ресурс]. – Режим доступа: http://www.dallaslock.ru/, свободный.

4. *Аппаратный комплекс СЗИ НСД "Аккорд-АМДЗ" на базе контроллера "Аккорд-5.5E"* [Электронный ресурс]. – Режим доступа: http://www.cbi-info.ru/groups/page-748.htm, свободный.

4. *«Аура» — система защиты информации от несанкционированного доступа (СЗИ от НСД)* [Электронный ресурс]. – Режим доступа: http://www.cobra.ru/prod/aura, свободный.

5. *Э. Мэйволд – Безопасность сетей, лекция 10 – Межсетевые экраны.* [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/102/102/lecture/2989, свободный.