**Министерство науки и высшего образования РФ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)**

Кафедра информатики и защиты информации

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РАДИОЭЛЕКТРОНИКИ

**ОТЧЕТ**

**по научно-исследовательской работе в семестре (НИР**)

«АЛГОРИТМЫ ВЫБОРА И ОПТИМИЗАЦИИ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ»

Шифр темы:

|  |  |  |
| --- | --- | --- |
| Исполнитель: |  |  |
| студент гр. ИСБ-119 | (подпись, дата) | Окунев В.В |

|  |  |  |
| --- | --- | --- |
| Научный руководитель: |  |  |
|  | (подпись, дата) | Полянский Д.А. |

|  |  |  |
| --- | --- | --- |
| Заведующий кафедрой: |  |  |
|  | (подпись, дата) | Монахов М.Ю. |

Владимир 2022

|  |
| --- |
| УТВЕРЖДАЮ |
| Заведующий кафедрой ИЗИ |
| \_\_\_\_\_\_\_\_\_\_\_\_М.Ю. Монахов |
| «\_\_\_» \_\_\_\_\_\_\_\_\_ 2021 г. |

**ЗАДАНИЕ**

на научно-исследовательскую работу в семестре студента Окунева В.В

4 курса, специальности группы

Предприятие ВлГУ

Последовательность прохождения НИР:

За время прохождения НИР необходимо:

Задание по стандартизации: отчёт должен быть выполнен в соответствии с ГОСТ 7.32-2001. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе, структура и правила оформления.

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель темы, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Полянский Д.А

к.т.н., доцент кафедры ИЗИ «\_\_» сентября 2022 г.

Исполнитель темы, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Окунев В.В

студент группы ИСБ-119 «\_\_» сентября 2022 г.

# РЕФЕРАТ

Отчёт на 24 стр., 6 рис., 6 таблиц, 7 источников.

Объектом исследования в данной работе являются программные средства защиты информации различных видов.

Целью данной работы является обеспечение адекватности выбора программных средств защиты информации в задаче построения комплекса средств защиты и разработка  алгоритма формирования исходных данных задачи выбора программных средств защиты информации

Задачи исследования: анализ предметной области, разработка общего алгоритма формирования исходных данных для решения задачи выбора комплекса средств защиты информации.

Результаты работы: Были рассмотрены различные программные СрЗИ, их сочетания и виды. Был выведен алгоритм расчета эффекта защиты каждого из средств для составления исходных данных задачи выбора комплекса СрЗИ.

Область применения: исследуемые подходы к определению эффективности СрЗИ для реализации мероприятий по обеспечению ИБ могут применяться для составления исходных данных при проектировании типовых задач выбора комплекса СрЗИ.

**Оглавление**

[РЕФЕРАТ 4](#__RefHeading___Toc979_4189451527)

[​ АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ. 5](#__RefHeading___Toc981_4189451527)

[​ АЛГОРИТМ ФОРМИРОВАНИЯ ИСХОДНЫХ ДАННЫХ ЗАДАЧИ ВЫБОРА ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 12](#__RefHeading___Toc989_4189451527)

[ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 24](#__RefHeading___Toc991_4189451527)

[ВЫВОД 25](#__RefHeading___Toc993_4189451527)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ. 26](#__RefHeading___Toc995_4189451527)

# АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ.

1. Введение

СрЗИ — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещественных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

* Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.
* Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).  
  Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
* Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

1. ОЦЕНКА ЭФФЕКТИВНОСТИ СрЗИ.

У каждого средства защиты информации есть определенные характеристики, типы назначения, использования, показатели эффективности, стоимость его производства, стоимость эксплуатации, особенности эксплуатации и прочее.

Одна из самых важных характеристик — показатель эффективности СрЗИ.

Для решения задачи по выбору СрЗИ нужно оценить эффективность СрЗИ.

Оценка эффективности средств защиты информации представляет собой непрерывный во времени процесс, и проводить её анализ имеет смысл только в динамике. На настоящий момент оценка эффективности средств защиты информации осуществляется на основе эксплуатационных и технических показателей. Эксплуатационные показатеsли, изложены в приказах ФСТЭК России об утверждении требований безопасности к информации, содержащейся в информационных системах различного назначения: государственных, для обработки персональных данных, для управления производственными технологическими процессами.

Технические показатели отражены в Профилях защиты для соответствующих видов средств защиты информации. Профиль защиты – это методический документ, представляющий собой совокупность задач защиты, функциональных требований, требований адекватности и их обоснование.

Эффективность функционирования средств защиты информации главным образом достигается квалифицированным и результативным управлением, следовательно, оценивая эффективность средств защиты информации в целом, целесообразно оценивать эффективность управления ими. На сегодняшний день существует множество способов оценки эффективности управления, в основе которых лежат оценка вероятности своевременного сбора всей необходимой информации для принятия решений, оценка квалификации персонала, принимающего решения и другие.

Однако, для решения данной задачи также подходит способ, позволяющий смоделировать значения части параметров средства защиты, которые невозможно измерить физически. При этом достаточной мерой оценки эффективности управления, является, как минимум, соответствие ее частных показателей оговоренным требованиям, тогда уровень эффективности управления при выполнении всех без исключения норм принимается за достаточный уровень эффективности. Оценка эффективности осуществляется в реальном масштабе времени. Исходными данными являются: частные показатели эффективности управления, нормативные значения, соответствующие каждому частному техническому и эксплуатационному показателю эффективности управления, сведения, полученные в процессе опроса экспертов в данной области знаний. В соответствии с выбранной стратегией оценки эффективности управления моделируют процессы управления средством защиты, подсчитывают статистические характеристики этих процессов управления, исходные данные оценивают по программе оценки эффективности управления, в процессе подсчёта обеспечивается свертка частных показателей эффективности управления, соответствующих результатам анализа измеряемых параметров, далее анализируют, отображают и документируют результаты оценки. В результате получается обобщенный показатель эффективности управления.

Таким образом достигается расширение функциональных возможностей системы защиты информации путём повышения точности оценки эффективности управления средствами защиты информации с помощью обеспечения моделирования значений части параметров, которые невозможно измерить физически.

Для эффективного обеспечения защиты информации требуется использовать комплекс СрЗИ, а не отдельные типы СрЗИ. Поэтому надо учитывать еще и их взаимодействие и вообще возможность взаимодействия.

Комплекс СрЗИ - совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Комплекс выбранных средств должен удовлетворять требованию максимального общего эффекта защиты. Эффект защиты всего комплекса прямо пропорционален эффекту отдельного

СрЗИ, а коэффициентом пропорциональности будет являться количество СрЗИ данного типа.

1. ОПИСАНИЕ ЗАДАЧИ ВЫБОРА КОМПЛЕКСА СрЗИ.

Под эффектом СрЗИ можно понимать количество угроз ИБ, которое оно может отразить в единицу времени или в определенных условиях   
Для того, чтобы выбрать оптимальный вариант комплекса СрЗИ можно использовать методы динамического программирования, так как ДП имеет обязательным атрибутом итерационность (многошаговость). Поэтому процесс принятия решения по выбору того или иного СрЗИ должен быть разделен на отдельные этапы.

В общем виде задача заключается в выборе некоторого кол-ва СрЗИ каждого из возможных типов в условиях заданного ограничения общего объема финансирования.

Задача выбора комплекса СрЗИ имеет 3 вида:

1. **неограниченная** (Комплекс СрЗИ может содержать средства любых типов в любом количестве при условии, что общая стоимость не превышает установленного предела. Минимальное количество средств каждого типа не ограничено (средство данного типа может вообще отсутствовать). Максимальное количество средств каждого типа ограничено только опосредованно через его стоимость и общий объём финансирования.)
2. **ограниченная** без обязательного применения (Комплекс СрЗИ может содержать средства любых типов в количестве не более заданного при условии, что общая стоимость не превышает установленного предела. Минимальное количество средств каждого типа не ограничено (средство данного типа может вообще отсутствовать). Максимальное количество средств каждого типа ограничено x i <= b i , где b i – заданные натуральные числа, указывающие максимальное количество СрЗИ каждого типа в комплексе. Данное ограничение обусловлено тем, что увеличение количества однотипных средств повышает общий эффект только до определённого предела, после которого средства становятся избыточными.)
3. **ограниченная** с обязательным применением. (Комплекс СрЗИ может содержать средства каждого типа в количестве не менее нижнего предела и не более верхнего при условии, что общая стоимость не превышает установленного предела. Минимальное количество средств каждого типа ограничено: <= , где – заданные натуральные числа, указывающие минимальное количество СрЗИ каждого типа в комплексе. Максимальное количество средств каждого типа также ограничено: <= , где – заданные натуральные числа, указывающие максимальное количество СрЗИ каждого типа в комплексе.)

# АЛГОРИТМ ФОРМИРОВАНИЯ ИСХОДНЫХ ДАННЫХ ЗАДАЧИ ВЫБОРА ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Для рассмотрения были выбраны следующие представители программных СрЗИ:

* Средства антивирусной защиты.
* Средства архивации информации
* Криптографические средства

Средства антивирусной защиты - программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Средства архивации информации – средства, позволяющие производить слияние нескольких файлов в один (в архив) с сокращением общего объема исходных файлов, путем устранения избыточности, но без потерь информации.

Средства криптографической защиты информации - специальные службы или программы, обеспечивающие шифрование и расшифрование информации с целью ее защиты от несанкционированной обработки, доступа и хранения при обмене ею по каналам связи, а также отвечающие за генерацию электронной подписи.

Описание алгоритма:

Требуется выбрать некоторое количество конкретных представителей данного вида средств защиты информации. Затем необходимо выбрать какие-то параметры (не менее 3-х), наиболее полно отражающие характеристики данного представителя СрЗИ. Эту операцию проделать с абсолютно с каждым средством. Затем необходимо привести разнородные параметры, у которых разные единицы измерения, к одинаковым условным единицам измерения. Это делается с помощью формул 1 и 2. Если наибольшее значение параметра является наилучшим, то следует выбрать формулу 1 для вычисления эффективности параметра СрЗИ. Если наоборот, то следует выбрать формулу 2.   
Затем следует заново сформировать табличные данные, с учетом перевода всех параметров к единым единицам измерения их эффективности. Желательно, визуализировать с помощью графиков табличные значения. Таким образом и получаются исходные данные для задачи выбора комплекса СрЗИ.

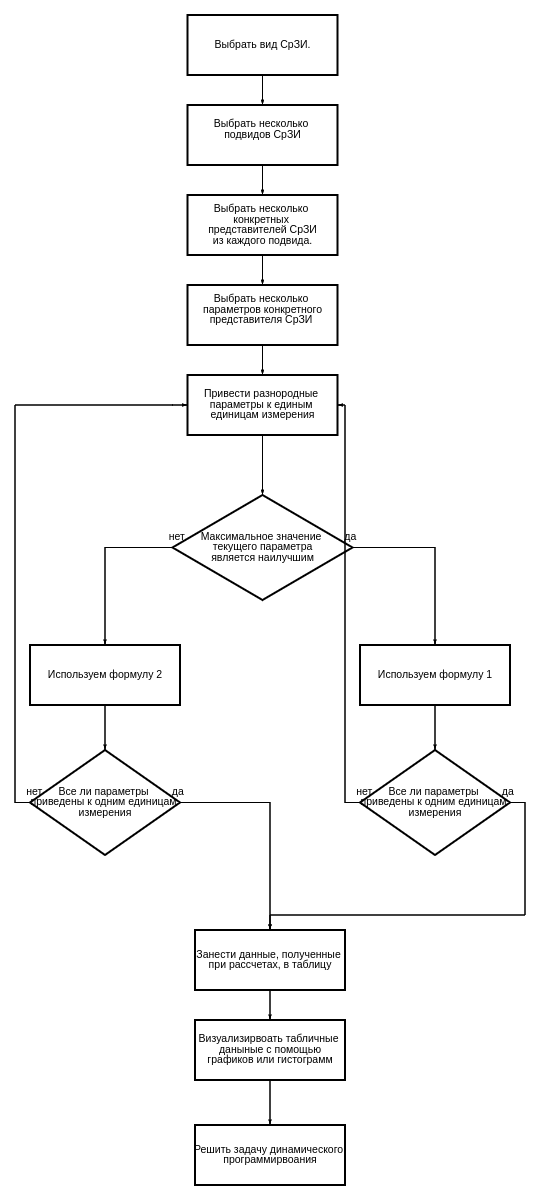


Рисунок 1 - «Блок-схема алгоритма»

Для рассмотрения были выбраны следующие представители средств архивации информации. У них были выделены определенные характеристики и занесены в таблицу.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых форматов архивов | Размер словаря | Максимальный размер поддерживаемых файлов. |
| WinRAR | 12 | 1024 мб | 16 эксабайт |
| 7ZIP | 44 | 512 мб | 16 эксабайт |
| PeaZIP | 200 | 256 мб | 16 эксабайт |

Средства антивирусной защиты.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых десктопных ОС | Стоимость покупки лицензии для 25 устройств на год | Минимальное количество оперативной памяти для работы. |
| Kaspersky | 3 | 28 700 р | 1024 мб |
| DrWEB | 3 | 32 582 р | 512 мб |
| ESET | 2 | 52 600 р | 128 мб |

Средства шифрования данных.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых десктопных ОС | Количество используемых алгоритмов шифрования | Цена |
| NordLocker | 2 | 3 | 4$ |
| AESCrypt | 3 | 1 | 0 |
| FILEVAULT | 1 | 2 | 0 |

Оцениваемые параметры разнородны и для их совместного использования в одной модели необходимо нормировать количественные данные с учетом их значимости. Нормирование, в частности, можно выполнить сведением к единичному интервалу вещественных чисел [0, 1] с учетом весовых коэффициентов при последующих преобразованиях.

Для нормирования необходимо ввести понятия минимальное, максимальное, наилучшее, наихудшее и оптимальное значение q-го параметра. Обозначим их соответственно xqMin , xqMAX ,xqНЛ xqНХ xqОПТ

Очевидно, что не всегда максимальное значение является наилучшим, а минимальное — наихудшим. Обычно для таких параметров как количество средств обеспечения какого-либо защищаемого свойства ИР максимальное — есть наилучшее. Для всех временных характеристик, количественных характеристик, определяющих точки доступа к ИР, а также затраты на приобретение или содержание СрЗИ максимальное — есть наихудшее.

Для нормирования будем использовать преобразования вида:

* для совпадения максимального и наилучшего значений параметра, которое оптимально с точки зрения организации СЗИ.



Рисунок 2 - формула 1

* Для совпадения минимального и наилучшего значений параметра, которое оптимально с точки зрения организации СЗИ.



Рисунок 3 - «формула 2»

Формула 1 будет использоваться при вычислении эффективности для следующих параметров: Количество поддерживаемых форматов архивов, Размер словаря, Максимальный размер поддерживаемых файлов, Количество поддерживаемых десктопных ОС, Количество используемых алгоритмов шифрования.

Формула 2 будет использоваться при вычислении эффективности для следующих параметров: Стоимость покупки лицензии для 25 устройств на год, Минимальное количество оперативной памяти для работы, Цена.

Вычисление эффективности каждого из параметров каждого из СрЗИ:

Winrar:

1-й параметр: = 0

2-й параметр: = 1

3-й параметр: = 0

7Zip:

1-й параметр: = = 0.17

2-й параметр: = 0.33

3-й параметр: = 0

PeaZip:

1-й параметр: = 1

2-й параметр: = 0

3-й параметр: = 0

Kaspersky:

1-й параметр: = 1

2-й параметр: = 1

3-й параметр: = 0

DrWeb:

1-й параметр: = 1

2-й параметр: = 0.84

3-й параметр: = 0.57

ESET:

1-й параметр: = 0

2-й параметр: = 1

3-й параметр: = 1

NordLocker:

1-й параметр: = 0.5

2-й параметр: = 1

3-й параметр: = 0

AESCrypt:

1-й параметр: = 1

2-й параметр: = 0

3-й параметр: = 1

FileVault:

1-й параметр: = 0

2-й параметр: = 0.5

3-й параметр: = 1

После произведения вычислений и приведения разнородных параметров СрЗИ к единой системе измерения были получены следующие таблицы и графическое представление табличных данных.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых форматов архивов | Размер словаря | Максимальный размер поддерживаемых файлов. |
| WinRAR (кр) | 0 | 1 | 0 |
| 7ZIP (зел) | 0.17 | 0.33 | 0 |
| PeaZIP (син) | 1 | 0 | 0 |

Таблица 4 - «Эффективность средств архивации информации»

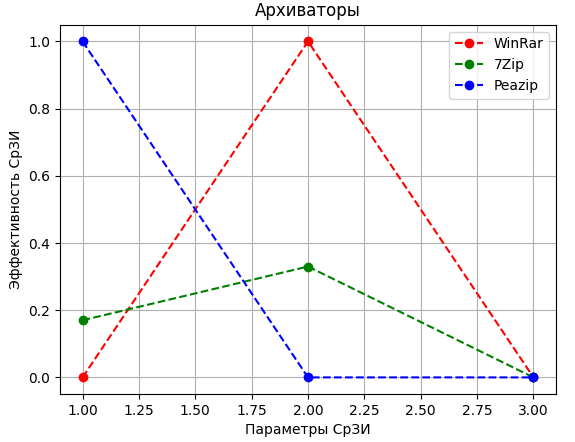


Рисунок 4 - «График эффективности средств архивации информации»

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых десктопных ОС | Стоимость покупки лицензии для 25 устройств на год | Минимальное количество оперативной памяти для работы. |
| Kaspersky (кр) | 1 | 1 | 0 |
| DrWEB (зел) | 1 | 0.84 | 0.57 |
| ESET (син) | 0 | 0 | 1 |

Таблица 5 - «Эффективность антивирусных средств защиты»

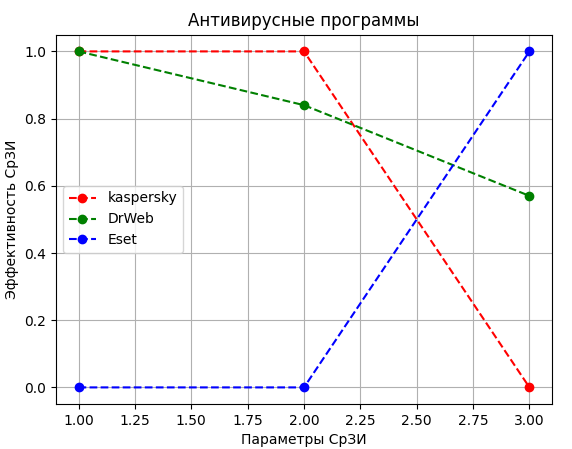


Рисунок 5 - «Эффективность антивирусных средств защиты»

|  |  |  |  |
| --- | --- | --- | --- |
|  | Количество поддерживаемых десктопных ОС | Количество используемых алгоритмов шифрования | Цена |
| NordLocker (кр) | 0.5 | 1 | 0 |
| AESCrypt (зел) | 1 | 0 | 1 |
| FILEVAULT (син) | 0 | 0.5 | 1 |

Таблица 6 - «Эффективность криптографических средств защиты»

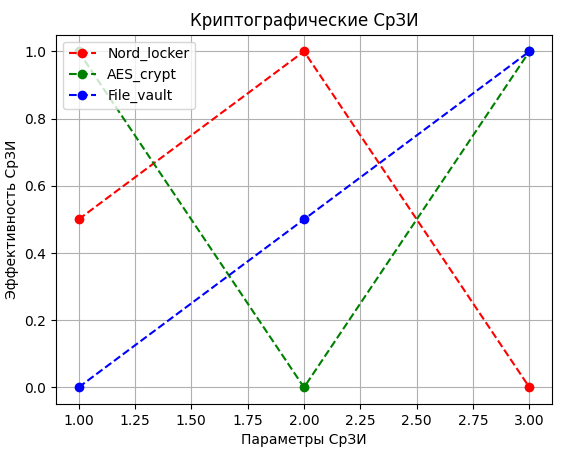


Рисунок 6 - «Эффективность криптографических средств защиты»

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчёте научно-исследовательской работы применяются следующие сокращения:

СрЗИ – средства защиты информации  
ИБ — информационная безопасность

АС – автоматизированная система

НСД – несанкционированный доступ

ИСПДН - информационная система персональных данных

# ВЫВОД

Решить задачу выбора комплекса СрЗИ методом динамического программирования несложно. Гораздо более сложная и важная задача – получение исходных данных для этой задачи. В ходе выполнения этой работы был разработан общий алгоритм формирования исходных данных для решения задачи выбора комплекса средств защиты информации. Точность решения задачи выбора комплекса СрЗИ прямым образом зависит от исходных данных, которые были получены.

# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ.

* https://it-security.admin-smolensk.ru/zinfo/szi/
* https://cyberleninka.ru/article/n/otsenka-effektivnosti-sredstv-zaschity-informatsii/viewer
* https://www.anti-malware.ru/analytics/Market\_Analysis/infosecurity-systems-classification-fsb-fstek
* <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty>
* <https://detsys.ru/catalog/sredstva_zashchity_peregovorov/podavitel_diktofonov/tf_012n_apparatura_zashchity_konfidentsialnykh_peregovorov/>
* <http://detektor.ru/>
* Д.А Полянский – Проведение экспертизы, Анализ и обработка данных в сфере информационной безопасности.