



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Оценка эффективности системы защиты информации



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Принципы проектирования СЗИ

Принцип системности предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИТКС.

Принцип комплексности предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Принцип непрерывности защиты предполагает, что защита информации - это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИТКС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Разумная достаточность предполагает следующее. Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности (например, с точки зрения цены информации).

Принцип гибкости (адаптивности) системы защиты на обеспечение возможности варьирования уровнем защищенности. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Принцип открытости алгоритмов и механизмов

защиты предполагает, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы СЗИ не должно давать возможности ее преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Принцип простоты применения средств защиты

заключается в том, что механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т. д.).



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Эффективность СЗИ оценивается как на этапе разработки, так и в процессе эксплуатации. В оценке эффективности СЗИ, в зависимости от используемых показателей и способов их получения, можно выделить три основных подхода: классический; официальный; экспериментальный.

Активно развивается и экономический подход.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Под **классическим** подходом к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной ИС. Такой подход используется при разработке и модернизации СЗИ. Однако возможности классических методов комплексного оценивания эффективности применительно к СЗИ ограничены в силу ряда причин.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Высокая степень неопределенности исходных данных, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев оптимальности создают значительные трудности для применения классических методов оценки эффективности. Для более подробного ознакомления можно **изучить** статью Марковой.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

- 1. Подход статистический:** конкретная угроза возникает в среднем за анализируемый период времени.
Способ расчета: статистическая обработка угроз и их последствий.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

2. Подход вероятностный: по формуле определяются суммарные средние потери. **Способ расчета:** определяется вероятность отказа системы от обработки персональных данных в результате реализации угроз.



3. Частотный подход: определяется ожидаемый ущерб от конкретной угрозы.
Способ расчета: на основании статистики задается показатель частоты возникновения угрозы и условный показатель ущерба. По формуле рассчитывается ожидаемый ущерб как функция указанных показателей.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

4. Экспертное оценивание: степень ИБ ИСПДн.

Способ расчета: определяется перечень параметров, характеризующих СЗИ; задаются значения субъективных коэффициентов важности каждой из характеристик, назначенных экспертным путем; рассчитывается их усредненное произведение.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

5. Информационно - энтропийный подход:
по формуле Шеннона.

Способ расчета: аналитическое вычисление
информационной энтропии, используя
понятие свертки функций.



6. Нейросетевой подход: нечеткие показатели защиты ИС в виде лингвистических переменных, таких как «абсолютно незащищенная», «недостаточно защищенная» и т.п.

Способ расчета: принадлежность определенного уровня ИБ определяется на заданном промежутке, показатели надежности являются функцией принадлежности к требованиям безопасности.



7. Метод минимизации рисков:

используется показатель экономического эффекта от управления рисками.

Способ расчета: производят фиксацию рисков; определяют у каждого индекс на основе затрат; задают способ обработки; рассчитывают показатели от управления рисками.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

8. Другие подходы: матричный, многоуровневый, оптимизационный

Обзор средств анализа защищенности

Наиболее известные программные продукты для анализа защищенности:

ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

- Nessus Security Scanner (www.nessus.org);
 - NetRecon 3.0+SU7 (www.axent.ru);
 - Internet Scanner (www.iss.net);
 - CyberCop Scanner (www.pgp.com);
 - HackerShield (www.bindview.com);
- Security Administrator's Research Assistant (SARA) (www.wwwarc.com/sara/);
- System Analyst Integrated Network Tool (SAINT) (www.wwdsi.com)
 - Retina (www.eeeye.com);
 - XSSprider (www.xspider.ru).



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Лучшие результаты показали два продукта: из бесплатных – Nessus Security Scanner, из коммерческих – Internet Scanner, выполняющие дистанционные проверки и работающие на уровне сети.

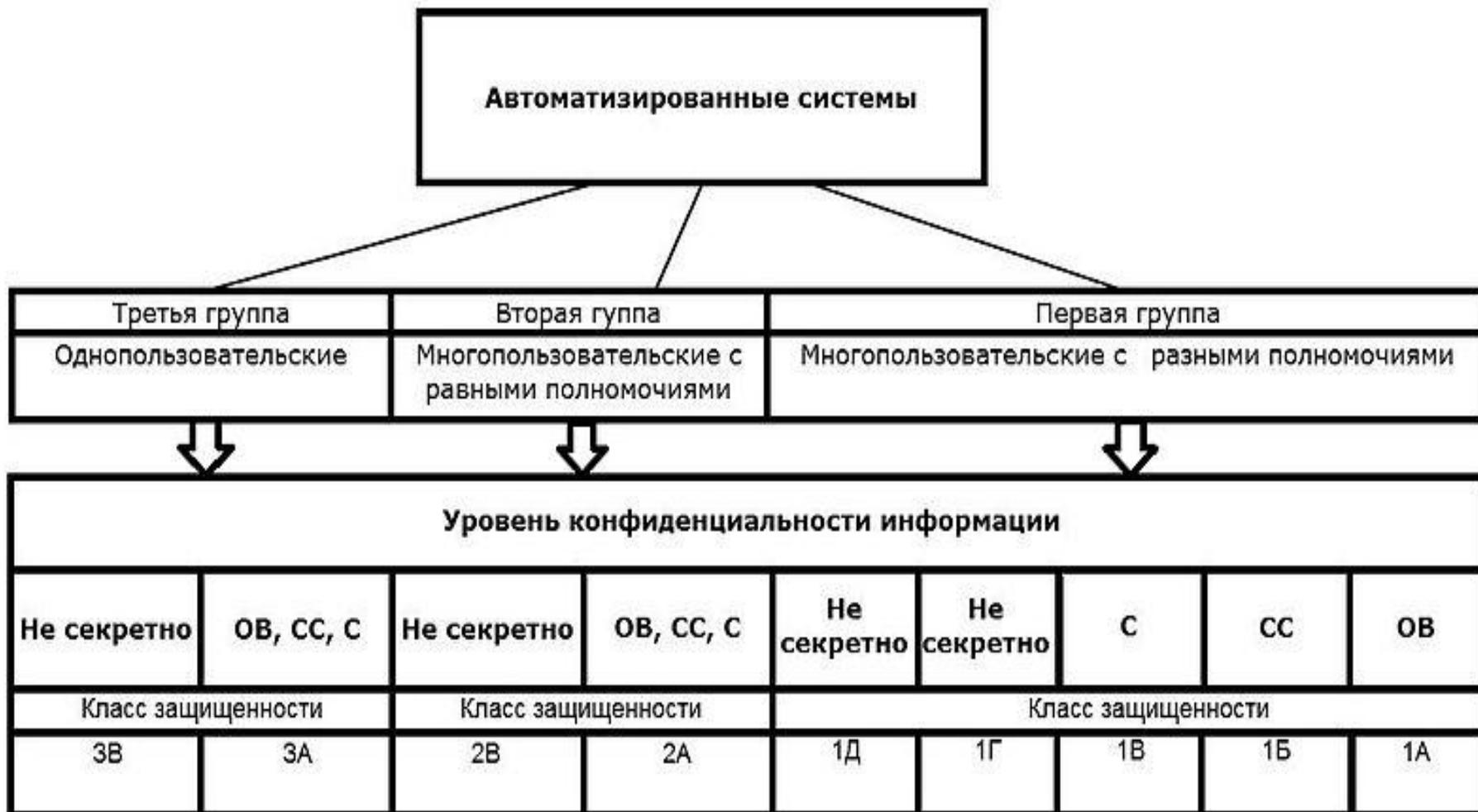


ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Большую практическую значимость имеет подход к определению эффективности СЗИ, который условно можно назвать **официальным**. Политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. В этих документах необходимо определить требования к защищенности информации различных категорий конфиденциальности и важности.



Классы защищенности АС





ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Требования по защите средств вычислительной техники и автоматизированных систем от НСД

Класс защищенности СВТ (АС) определяется совокупностью показателей (требований) защищенности.

Для СВТ рассматривается 21 показатель защищенности. Показатели выбираются разработчиками СЗИ.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Под **экспериментальным** подходом понимается организация процесса определения эффективности существующих СЗИ путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников. Такие исследования проводятся следующим образом. В качестве условного злоумышленника выбирается один или несколько специалистов в области информационной борьбы наивысшей квалификации.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению слабых звеньев в системе защиты. При этом могут моделироваться действия злоумышленников, соответствующие различным моделям поведения нарушителей: от неквалифицированного злоумышленника, не имеющего официального статуса в исследуемой ИС, до высококвалифицированного сотрудника службы безопасности.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Экономический подход к защите информации включает:

- Изучение вопросов экономической оценки информационных ресурсов.**
- Получение знаний о методах оценки угроз и степени риска в деятельности предприятия.**
- Знакомство с технико-экономическими задачами обеспечения ИБ.**
- Формулирование и решение задач создания экономически обоснованных систем ИБ предприятия.**



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Экономическая задача создания системы ИБ предприятия

Задача может формулироваться исходя из возможностей предприятия или заданной эффективности системы:

- 1. При заданном объеме расходуемых ресурсов обеспечить достижение максимально возможного результата.**
- 2. Обеспечить достижение заданного результата при минимальном расходе необходимых ресурсов.**



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Экономическая оценка эффективности информационного обеспечения

Оценка экономической эффективности информационного обеспечения производится по двум составляющим:

1-я-по экономии времени руководителей и специалистов, занятых подготовкой решений;

2-я-по экономии, обусловленной использованием полученных научно-технических материалов.

За основу принимаются нормативные трудозатраты, с точки зрения потребителя информации.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Тогда, **экономия по первой составляющей за год** можно подсчитать по формуле:

$$Э_t = 0,545 (\Delta t_d * Z_{ср.д} * N_d + \Delta t_i * Z_{ср.и} * N_i),$$

где **0,545** - отношение числа месяцев в году к среднему числу рабочих дней в месяце;

Δt_d - экономия времени руководителей за счет информационного обеспечения (дней в месяц);

$Z_{ср.д}$ - среднемесячная зарплата одного руководителя, обеспечиваемого информацией (руб.);

N_d - число руководителей, получивших информацию и принявших ее к использованию;

Δt_i ; $Z_{ср.и}$; N_i - то же для специалистов, обеспечиваемых информацией и принимающих участие в подготовке решений.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Экономия затрат на разработку и внедрение научно-технических достижений по информационным материалам (**Эз**) можно рассчитать по формуле

$$\mathbf{Эз = В_1 - (В_2 - В_р)}, \text{ где,}$$

В₁ - затраты на разработку достижений при отсутствии информации (техдокументации);

В₂ - затраты на доработку достижений при их внедрении;

В_р - расходы на получение техдокументации.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Обозначим время, необходимое на собственную разработку новшества - T_p , тогда выигрыш во времени за счет использования материалов НТИ составит:

$$I = T_p - (T_v + t_{\text{инф}}),$$

где T_v - время внедрения новшеств;

$t_{\text{инф}}$ - время, затраченное на информационные процессы.

Годовой экономический эффект от ускорения реализации экономического потенциала новшеств

определяется годовой экономией $\mathcal{E}_T = E_n * \mathcal{E}_n * I$, где

E_n - нормативный коэффициент эффективности капитальных вложений;

\mathcal{E}_n - потенциальный экономический эффект заложенный разработчиками.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Доля экономии, приходящейся на информационную службу (**Эи**), определяется по формуле:

$$\mathbf{Эи = \frac{Эн - Зи}{Зр.в},}$$

где **Эн** - годовая экономия от использования новых

технических средств, созданных при участии службы ИТИ;

Зи - годовой фонд зарплаты штатных и внештатных сотрудников информационной службы;

Зр.в - годовой фонд зарплаты специалистов, занятых разработкой и внедрением новшеств.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Тогда **суммарный годовой эффект** информационного обеспечения (**Энти**) с учетом составляющих экономии, рассмотренных выше, определяется как:

$$\mathbf{Энти} = \mathbf{Эт} + \mathbf{Эз} + \mathbf{Эт} + \mathbf{Эи} - (\mathbf{Снти} + \mathbf{Ен} * \mathbf{Кнти}),$$

где **Снти** - себестоимость информационных работ, включающая текущие затраты на их проведение;

Кнти - капитальные вложения в информационную систему.



ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Интеллектуальная собственность

Промышленная собственность:

Изобретения
Полезные модели
Промышленные образцы
Товарные знаки
Знаки обслуживания
Фирменные наименования
Указания происхождения
или наименования
места происхождения
Пресечение
недобросовестной
конкуренции

Авторские права:

Литературные
произведения
Драматические и
музыкально-драматические
произведения
Аудио- визуальные
произведения
Радиопроизведения
Произведения
изобразительного
искусства
Произведения
прикладного искусства
Программы для ЭВМ
Базы данных

Смежные права:

распространяются на
постановки,
исполнения, звуко- и
видеозаписи
исполнения,
фонограммы, передачи
организаций эфирного
и кабельного вещания,
**сопровождение
баз данных**