Некоммерческое акционерное общество

Кафедра
Систем информационной безопасности

ОЦЕНКА РИСКОВ И АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания по выполнению расчетно-графических работ для студентов специальности 5В100200 – Системы информационной безопасности.

Алматы 2017

СОСТАВИТЕЛЬ: М.В. Дмитриева. Оценка рисков и аудит систем информационной безопасности. Методические указания по выполнению расчетно-графических работ для студентов специальности 5В100200 – Системы информационной безопасности. – Алматы; АУЭС, 2017 – 18 с.

Методические указания предназначены для студентов очной формы обучения и содержат общие положения по выполнению расчетно-графических работ. Приводится рекомендуемая литература.

Ил. 1, табл. 5, библогр. – 7 назв.

Рецензент: доц. Ю.М. Гармашова

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2017 г.

Сводный план 2017 г., поз. 117

Маргарита Валерьевна Дмитриева

ОЦЕНКА РИСКОВ И АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания по выполнению расчетно-графических работ
для студентов
специальности 5В100200 – Системы информационной безопасности

Редактор _____
Специалист по стандартизации Н.К. Молдабекова

Подписано в печать ___.___.___ Формат 60х84 1/16
Тираж 50 экз. Бумага типографская №1
Объем 0,9 уч.-изд. л. Заказ ___ Цена 450 *тг.*

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013 Алматы, Байтурсынова, 126

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ
Кафедра систем информационной безопасности

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ С.В. Коньшин
«____» _____ 201_ г.

ОЦЕНКА РИСКОВ И АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания по выполнению расчетно-графических работ
для студентов
специальности 5В100200 – Системы информационной безопасности

СОГЛАСОВАНО
Начальник УМО
_____ Р.Р. Мухамеджанова
«____» _____ 201_ г.

Председатель ОУМЛ по МО и Э
_____ Б.К. Курпенов
«____» _____ 201_ г.

Редактор
_____ _____
«____» _____ 201_ г.

Специалист по стандартизации
_____ _____
«____» _____ 201_ г.

Рассмотрено и одобрено на
заседании кафедры СИБ
Протокол №_ от «__» _____ 201_ г.
Зав. кафедрой _____ Р.Ш. Бердибаев

Составитель
Ст. преподаватель кафедры СИБ
_____ М.В. Дмитриева

Содержание

Введение

Целью расчетно-графических работ является ознакомление студентов с базовой основой проектирования комплексных систем информационной безопасности.

Главной целью любой системы защиты является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений.

Расчетно-графические работы направлены на формирование у студентов систематизированного представления о принципах, методах и средствах реализации систем информационной безопасности. Они предназначены для изучения принципов организации и функционирования систем информационной безопасности.

Расчетно-графическая работа №1 посвящена методам оценивания информационных рисков организации. Рассматриваются табличные алгоритмы, а также приводятся расчеты по оценке информационных рисков.

Объектом исследования при выполнении РГР являются информационные риски, а предметом – расчет рисков информационной безопасности. Целью работы – изучение методик расчета рисков информационной безопасности.

Реализация намеченной цели потребует постановки и решения таких задач, определивших логику и концепцию исследования, как рассмотрение теоретических основ анализа рисков информационной безопасности и изучения показателей и алгоритмов расчета рисков по угрозам информационной безопасности.

Расчетно-графическая работа №2 посвящена организации и проведению аудита систем информационной безопасности организации. Рассматриваются подходы к практической реализации аудита.

В ходе выполнения данной расчетно-графической работы обучающимися будут получены первоначальные знания в области аудита информационной безопасности, приобретены навыки применения программно-технических средств контроля выполнения требований политики безопасности организации.

Тематика данных РГР относится к основным понятиям информационных рисков и аудита систем информационной безопасности и обеспечивают теоретическую базу для широкого круга практических задач.

1 Расчетно-графическая работа № 1. Расчет рисков системы информационной безопасности

Цель РГР (оценивания рисков): в определение базовых составляющих информационных рисков системы, обеспечивающей функционирование производственных процессов компании, а также ее ресурсов. После выполнения оценки рисков могут быть выбраны средства обеспечения требуемого в компании уровня информационной безопасности. В процессе работы с рисками рекомендуется учитывать следующие параметры для оценки: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты.

1.1 Задание А

Проработать последовательность действий, необходимых для проведения анализа информационных рисков. Оформить отчет.

Выбор варианта специфики организации из приложения А (вариант – номер по списку в журнале преподавателя; вариант – выбор самого студента или студент может предложить свою тему с необходимым и достаточным обоснованием ее целесообразности).

1.2 Методические указания к выполнению задания А

Анализ риска необходимо выполнять, непосредственно опираясь на цели и задачи по оптимизации защиты конкретных типов конфиденциальной информации.

Одной из важных задач при организации системы комплексного обеспечения информационной безопасности является обеспечение защиты данных с точки зрения целостности и доступности. При анализе учитывайте, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин таких, как:

– сбои оборудования, ведущие к потере или искажению информации;

– физические воздействия, возникающие как результат природных явлений;

– ошибок в используемом программном обеспечении (в том числе недокументированных возможностей).

Потому рациональнее под значением термина «атака» понимать как воздействия на информационные ресурсы компании со стороны людей, так и окружающей среды, в которой функционирует сама информационная система.

На рисунке 1 представлены все шесть шагов анализа риска (каждый из них должен планомерно детализироваться в каждом конкретном случае для той или иной компании).

Результаты, полученные в процессе оценивания рисков, должны быть представлены в виде, который удобен для их эффективного восприятия и выбора решений по улучшению имеющийся системы информационной безопасности. Следует помнить о том, что практически на любой информационный ресурс могут быть направлены воздействия нескольких потенциальных для него угроз.

Значение расчетной величины информационного риска для каждого ресурса определяется как произведение вероятности реализации угрозы, вероятности нападения на этот ресурс и потенциального ущерба от реализации атаки.

Рисунок 1 – Последовательность действий при анализе информационных рисков организации

1.3 Контрольные вопросы

1. Каково место анализа рисков при проектировании комплексных систем информационной безопасности?

2. Раскройте смысловое и характеристическое наполнение термина «атака».

3. Объясните, на что влияет величина риска, полученная при анализе рисков?

4. Перечислите основные задачи оценивания рисков. В чем их общность?

5. Какая рекомендуется последовательность реализации защиты информационных объектов?

6. Что означает мера обеспечения информационной безопасности?

7. Какие имеются характеристики мер обеспечения информационной безопасности?

8. Какова цель и основные функции анализа рисков информационной безопасности?

1.4 Задание В

Выполнить по выданному заданию:

1) Идентификацию рисков.
2) Оценку и расчет рисков.
3) Приоритезацию рисков.
4) Выбрать меры по обработке рисков.
5) Составить план по обработке рисков.
6) Оформить отчет.

1.5 Методические указания к выполнению задания В

Табличные методы оценки рисков.

В настоящее время известно множество табличных методов оценки информационных рисков компании. Рассмотрим несколько примеров подобных методов оценивания рисков, которые рекомендованы международными стандартами информационной безопасности, начиная с BS 7799. В 2013 году в Казахстане принят стандарт СТ РК ISO/IEC 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности», где приведены рекомендации по рекомендуемым методам оценки рисков информационной безопасности.

Существенно, что в этих рекомендуемых методах [1,2] количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса, то есть количественными методами. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть при помощи определения затрат на их приобретение или восстановление количественными методами.

Если обнаружится, что какое-либо прикладное программное обеспечение имеет особые требования к конфиденциальности или целостности, например, исходный текст имеет высокую коммерческую

ценность, то оценка этого ресурса производится в стоимостном выражении по той же схеме, что и для информационных ресурсов.

Количественные показатели информационных ресурсов рекомендуется оценивать по результатам опросов сотрудников компании – владельцев информации, то есть должностных лиц организации, которые могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий, вплоть до рассмотрения потенциальных воздействий на бизнес-деятельность организации при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении.

При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов компании, учитывающих:

– безопасность персонала;

– разглашение частной информации;

– требования по соблюдению законодательных и нормативных положений;

– ограничения, вытекающие из законодательства;

– коммерческие и экономические интересы;

– финансовые потери и нарушения в производственной деятельности;

– общественные отношения;

– коммерческую политику и коммерческие операции;

– потерю репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные – где количественные оценки по ряду причин затруднены.

При этом наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных для этих целей балльных шкал, подобных той, которая приводится далее: четырехбальная шкала от 1 до 4 баллов.

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанной с ним группе ресурсов оцениваются уровни угроз как вероятность реализации угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию.

Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале «высокий-низкий». Необходимую информацию собирают, опрашивая ТОР-менеджеров компании, сотрудников коммерческих, технических, кадровых и сервисных служб, выезжая на места и анализируя документацию компании.

П р и м е р.

Проведем анализ следующих типов угроз:

– умышленные несанкционированные действия людей;

– непредвиденные случайности;

– ошибки со стороны персонала;

– аварии оборудования, программного обеспечения и средств связи.

Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, показателям угроз и уязвимостей, оцениваются при помощи таблицы, аналогичной таблице 1.

Количественный показатель риска определяется в шкале от 1 до 8. Соответствующие значения заносятся в таблицу. Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Если существует уязвимость без связанной с ней угрозой или существует угроза, не связанная с какими-либо уязвимыми местами, то рисков нет. Но и в этом случае следует предусмотреть изменение положения дел. Каждая строка в таблице определяется показателем ресурса, а каждый столбец – степенью опасности угрозы и уязвимости. Например, ресурс имеет показатель 3, угроза имеет степень «высокая», а уязвимость – «низкая». Показатель риска в данном случае будет 5. Размер таблицы, учитывающей количество степеней опасности угроз, степеней опасности уязвимостей и категорий ценности ресурсов, может быть изменен в соответствии со спецификой конкретной компании.

Таблица 1 – Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей

Показатель ценности ресурса (на каждую угрозу и ресурс)	Уровень угрозы (оценка вероятности ее осуществления)								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
П р и м е ч а н и е – Н - низкий, С - средний, В - высокий.									

Описанный подход определяется классификацией рассматриваемых рисков. После того как оценивание рисков было выполнено первый раз, его результаты целесообразно сохранить, например, в базе данных. Эта мера в дальнейшем позволит легко повторить последующее оценивание рисков компании.

Ранжирование угроз.

В матрице или таблице можно наглядно отразить связь между угрозами, негативными воздействиями и возможностями реализации. Для

этого нужно выполнить следующие шаги (таблица 2). На первом шаге оценить негативное воздействие по заранее определенной шкале, например, от 1 до 5 для каждого ресурса, которому угрожает опасность (колонка *b* в таблице). На втором шаге по заранее заданной шкале, например, от 1 до 5, оценить реальность реализации (колонка с в таблице) каждой угрозы (колонка *a* в таблице). На третьем шаге вычислить показатель риска при помощи перемножения чисел в колонках *b* и *c*, по которому и производится ранжирование угроз (колонка *e*). В этом примере для наименьшего негативного воздействия и для наименьшей реальности реализации выбран показатель 1.

Таблица 2 – Ранжирование угроз

Описание угрозы	Показатель негативного воздействия	Реальность реализации угрозы	Показатель риска	Ранг угрозы
a	*b*	*c*	*d*	*e*
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Оценивание показателей частоты повторяемости и возможного ущерба от риска.

Рассмотрим пример оценки негативного воздействия угрозы. Эта задача решается при помощи оценивания двух значений: ценности ресурса и частоты повторяемости риска. Перечисленные значения определяют показатель ценности для каждого ресурса. Вначале каждому ресурсу присваивается определенное значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам.

После того, как баллы всех ресурсов анализируемой корпоративной системы будут просуммированы, определяется количественный показатель риска для системы. Далее оценивается показатель частоты повторяемости. Частота зависит от вероятности возникновения угрозы и степени легкости, с которой может быть использована уязвимость. В результате получим таблицу, аналогичную таблице 3.

Таблица 3 – Показатель частоты повторяемости риска

Уровень угрозы								
Низкий Уровни уязвимостей			Средний Уровни уязвимостей			Высокий Уровни уязвимостей		
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Затем определяется показатель пары ресурс/угроза. На каждую пару ресурс/угроза составляется таблица (таблица 4), в которой суммируются показатели ресурса и угрозы.

На заключительном этапе суммируются все итоговые баллы по всем ресурсам системы и формируется ее общий балл. Его можно использовать для выявления тех элементов системы, защита которых должна быть приоритетной.

Таблица 4 – Показатели пары ресурс/угроза

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Разделение рисков на приемлемые и неприемлемые.

Дополнительный способ оценивания рисков состоит в разделении их только на допустимые и недопустимые. Возможность применения подобного подхода основывается на том, что количественные показатели рисков используются только для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Таблица, используемая в данном подходе, содержит не числа, а только символы: Д (риск допустим) и Н (риск недопустим) – см. таблицу 5.

Таблица 5 – Разделение рисков на допустимые и недопустимые

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

1.6 Контрольные вопросы

1. Каковы принципы количественных и качественных подходов к оценке рисков?
2. Обоснуйте применение количественных и качественных алгоритмов при оценке рисков.
3. Объясните назначение и принципы использования бальных шкал.
4. Как определяется показатель пары ресурс/угроза?
5. Что такое количественный показатель риска для системы?

6. Как наглядно отразить связь между угрозами, негативными воздействиями и возможностями реализации?

7. В чем заключается дополнительный способ оценивания рисков и каково его предназначение?

8. Какие меры предусматриваются по обработке рисков? Сколько их?

2 Расчетно-графическая работа № 2. Организация аудита системы информационной безопасности

Цели РГР2:

1) Ознакомиться с возможностями и областью применения, а также получить навыки практического использования программно-технических средств контроля реализации требований безопасности, изложенной в политике безопасности компании.

2) Используя полученные практические результаты, выполнить планирование и задокументировать области проверки в процессе аудита информационной безопасности ранее (при выполнении РГР1) выбранной компании.

3) Получить навыки в создании рабочей и отчетной документации по итогам выполненного аудита.

Требования к выполнению:

1) Ознакомьтесь со структурой информационной среды выбранной компании.

2) При формировании отчета по выполнению данной работы придерживайтесь четкой структуры изложения материала.

2.1 Задание

1 Ознакомьтесь с выбранными средствами инструментального контроля:

а) изучите возможности данного средства контроля;

б) выполните мониторинг сети/компьютеров, установленных в учебной аудитории;

в) сформируйте один или несколько отчётов, включив в них предложения по устранению обнаруженных в процессе проверки несоответствий.

2 Подготовьте план мероприятий по аудиту информационной безопасности:

а) выбор областей информационной среды компании для проведения аудита;

б) используя один из стандартов информационной безопасности, сформулируйте ряд требований аудита;

в) разработка плана мероприятий с указанием проверяемых подразделений, сроков реализации и видов проверок.

3 Разработайте по результатам аудита итоговый отчёт:

а) выполнить анализ результатов аудита, предложив простейшую методику анализа;

б) разработать форму для аудиторского отчёта с указанием сотрудников, его заполняющих, и плана выполнения повторных проверок.

П р и м е р ы вариантов модификаций компаний (базовый профиль задания – тематика по курсовому проектированию)**:**

1) В компании четыре представительства, все в разных странах, в каждом от 50–100 сотрудников. Головная компания 1000 сотрудников в РК. Имеются несколько отделов (например, отдел продаж, административный отдел и отдел логистики).

2) Компания имеет одно представительство в РК, которое является компанией, купленной годом ранее. Головная компания до 300 чел. Представительство – до 100 сотрудников (например, разные бренды. Два домена – два бренда).

3) Компания имеет головной офис со штатом 300 сотрудников. По всему РК 2000–3000 представительств (например, представительства компании в магазинах. Имеется управляющий менеджер, тарифный отдел и отдел логистики).

4) Компания – 200 сотрудников. Клиенты в ряде стран мира. Компания обеспечивает поддержку инфраструктуры клиента (например, услуги аутсорсинга).

5) Компания состоит из трех филиалов на территории РК. Центральный офис в Алматы. Его численность 100 сотрудников, в филиалах 20 сотрудников. (например, занимается производством и разработкой средств аутентификации – производство в филиалах).

2.2 Методические указания к выполнению задания

Аудит информационной безопасности – это системный процесс получения объективных оценок текущего состояния информационной безопасности организации в соответствии с определенными критериями информационной безопасности, включающий обследование различных сред функционирования информационно-технической среды, тестирование ее на уязвимости, анализ и оценку защищенности, формирование отчета и разработку соответствующих рекомендаций.

Аудит информационной безопасности необходим для того, чтобы:

– получить оценку текущего состояние системы информационной безопасности компании;

– сформировать входные данные для постановки требований при реализации комплексной системы защиты информации, а также при ее модернизации.

Такой подход к реализации защиты позволит минимизировать использование злоумышленниками выявленных уязвимостей и оптимально обеспечит эффективную защиту информации в компании от несанкционированного доступа, изменений и/или уничтожения информационных ресурсов.

В общем случае аудит информационной безопасности включает в себя комплексное обследование различных сред функционирования информационной системы компании, тестирование ее на уязвимости, анализ и систематизацию полученных результатов, оценку уровня защищенности, формирование отчета и разработку соответствующих рекомендаций.

На этапе комплексного обследования проводится: обследование вычислительной системы, обследование информационной и физической среды, среды пользователей, тестирование на уязвимости.

В ходе проведения аудита системы информационной безопасности компании проверяется:

– наличие документации на ИТС и ее компоненты;

– наличие распорядительных документов на ИТС;

– общая структурная схема ИТС и ее состав (перечень и состав оборудования, технических и программных средств, их связи, особенности конфигурации, архитектуры и топологии, программные и программно-аппаратные средства защиты информации, взаимное размещение средств);

– виды и характеристики каналов связи;

– особенности взаимодействия компонентов ИТС;

– возможные ограничения относительно использования средств.

Кроме того, при обследовании вычислительной системы ИТС должны быть выделены компоненты, которые являются средствами защиты информации или содержат механизмы защиты, а именно: должны быть описаны потенциальные возможности этих средств и механизмов, их свойства и характеристики, в том числе те, которые устанавливаются по умолчанию.

Проведение квалифицированного аудита информационной безопасности и исполнение комплекса мер по защите информационных ресурсов по рекомендациям, выработанным в результате такого аудита, дает уверенность в защищенности ИТС на определенный период. Но высокие технологии развиваются динамично, и вместе с ними совершенствуются средства совершения преступлений в сфере ИТ. Поэтому аудит информационной безопасности следует проводить периодически и на более технологически совершенном уровне. Уверенность в защищенности информационных ресурсов может быть обоснована только тогда, когда она подтверждена.

2.3 Контрольные вопросы

1. Каково место аудита при проектировании комплексных систем информационной безопасности?
2. Что входит в полную характеристику термина «комплексный аудит»?
3. Объясните, для каких целей используется информация, полученная в процессе выполнения аудита?
4. На что влияет отличие видов аудиторских доказательств?
5. В чем заключается контроль качества проведения аудиторской проверки?
6. Что такое методы аудиторского контроля?
7. Как выполняется регулирование аудиторской деятельности?
8. Перечислите целевое назначение и функции внутреннего и внешнего аудита. Что общего и в чем различие?

Приложение А

Таблица 1 – Варианты заданий

№	*Организация*	*№*	*Организация*
1	Департамент коммерческого банка	16	Офис благотворительного фонда
2	Медицинское учреждение	17	Издательство
3	Колледж	18	Консалтинговая фирма
4	Офис страховой компании	19	Рекламное агентство
5	Рекрутинговое агентство	20	Отделение налоговой службы
6	Интернет-магазин	21	Офис нотариуса
7	Центр обслуживания населения	22	Бюро перевода (документов)
8	Отделение полиции	23	Научно проектное предприятие
9	Страховая компания	24	Редакция газеты
10	Дизайнерская фирма	25	Гостиница
11	Офис интернет-провайдера	26	Городской архив
12	Аэропорт	27	Фармацевтическая фирма
13	Компания по разработке ПО для сторонних организаций	28	Автосалон
14	Агентство недвижимости	29	Пенсионный фонд
15	Туристическое агентство	30	Магазин

Список литературы

1 ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management.

2 СТ РК ISO/IEC 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

3 Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – М.: Мастер систем, 2003.

4 Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.

5 Ярочкин В.И. Безопасность информационных систем. – М.: Ось-89, 1989.

6 Петраков А.В. Основы практической защиты информации. Учебное пособие. – Радио и связь, 2013.

7 Гундарь К.Ю. , Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – Киев: «Корнейчук», 2000.