Цель работы

Изучение методов декомпозиции активов систем на компоненты информационных взаимодействий, получение навыков анализа защищенности ресурсов и численной оценки рисков с помощью модели информационных потоков и модели угроз/уязвимостей..

Вариант задания – 1. Тестовая КИС *«ТестИС-Софт»*.

Компания *«ТестИС-Софт»* разрабатывает программное обеспечение для финансовых организаций.

Руководство компании представлено генеральным директором. Штат компании – 150 человек.

Все разработки компании носят закрытый характер. Для поддержания процессов и контроля используемых ресурсов в штатном расписании предусмотрены следующие должности: главный администратор, администратор файловых серверов, сетевой администратор. Остальные сотрудники – аналитики, инженеры по разработке ПО, тестировщики, разработчики и руководители проектов. В бухгалтерии работает один сотрудник – главный бухгалтер. База данных бухгалтерии находится на его рабочей станции. Информация, обрабатываемая в системе – результаты и данные разработки программных продуктов: аналитические данные, технические задания, документация на системы заказчиков, исходные коды, программная документация, исполняемые модули, результаты тестирования.

В компании используется антивирусная защита, все серверы расположены в серверном помещении, запираемом на ключ. На серверах установлены системы контроля версий; почтовый и файловый серверы защищены межсетевым экраном. Сервер системы контроля версий доступен тестировщикам из сети. Интернет по VPN-соединению. Компьютер главного бухгалтера не имеет дисководов и устройств подключения USB, кроме того, он не включен в основную сеть. Резервное копирование не производится. Дирекция и руководители проектов имеют доступ в сеть Интернет с рабочих мест. Только разработчики могут вносить изменения в системе контроля версий.

Ход работы

В рассматриваемом примере КИС выделены следующие ресурсы: почтовый и файловый серверы, защищенные МЭ; рабочие станции разработчиков; рабочие станции тестировщиков; рабочие станции дирекции и руководителей проектов; компьютер главного бухгалтера; сервер системы контроля версий.

Были определены следующие группы пользователей: главный бухгалтер, главный администратор, администратор файловых серверов, сетевой администратор, аналитики, тестировщики, разработчики, руководители проектов, руководство компании. В *таблице 1* приведены выделенные примеры групп пользователей и видов доступа.

Таблица 1 – Информационные потоки

Группа пользователей	**Информация**	**Пользователей в группе**	**Права доступа**	**Вид доступа**	**Закрытый канал**
Главный бухгалтер	База данных бухгалтерии	1	все	локальный	да
Главный администратор	Интернет	1	все	удаленный	да
	Почтовый и файловый серверы				
Администратор файловых серверов	Интернет	1	все	удаленный	нет
	Файловый сервер				да
Сетевой администратор	Интернет	1	все	удаленный	нет
	Почтовый сервер				да
Аналитики	Интернет	35	чтение	удаленный	нет
	Система контроля версий				да
Тестировщики	Интернет	28	чтение	удаленный	нет
	Система контроля версий				да
Разработчики	Интернет	73	все	удаленный	нет
	Система контроля версий				да
Руководители проектов	Интернет	7	все	удаленный	нет
Руководство компании	Интернет	3	все	удаленный	нет

Средства защиты информации на серверах: физический контроль доступа в помещение (отдельные серверные помещения, двери с замками), межсетевой экран, VPN.

Средства защиты компьютера главного бухгалтера: отсутствие дисководов и устройств подключения USB, ограничение доступа в основную сеть.

Средства защиты остальных рабочих мест: ограничение доступа сотрудников в сеть Интернет, ограничение доступа к системе контроля версий, антивирусные средства.

Весовые коэффициенты для существующих средств защиты представлены в *таблице 2.*

Таблица 2 – Весовые коэффициенты средств защиты ИС

Средство защиты	**Вес**
Средства физической защиты	
Контроль физического доступа в помещение, где расположен ресурс	15
Средства локальной защиты	
Антивирусное ПО	10
Отсутствие дисководов и USB-портов	12
Ограничение на полный доступ к основной сети	5
Средства персональной сетевой защиты	
Доступ по VPN	10
Межсетевые экраны	5

В *таблице 3* представлена оценка ущерба от нарушений безопасности.

Таблица 3 – Оценка ущерба компании от нарушений безопасности

Информация	**Конфиденциальность (у.е. в год)**	**Целостность (у.е. в год)**	**Доступность (ч)**
База данных бухгалтерии	300	300	2
База данных системы контроля версий	300	300	2
Почтовый и файловый серверы	400	100	5

Рассчитаем риск по угрозе конфиденциальности информации. При локальном доступе к информации на ресурсе необходимо найти коэффициент локальной защищенности информации на ресурсе, который представляет сумму весов средств физической и локальной защиты.

При удаленном доступе рассчитываются коэффициенты локальной защищенности рабочего места группы пользователей, имеющей доступ к информации (сумма весов средств физической, локальной и персональной сетевой защиты) и удаленной защищенности информации на ресурсе (сумма весов средств корпоративной сетевой защиты). При локальном и удаленном доступе находим все три коэффициента, из которых выбирается наименьший. Результаты представлены в *таблице 4*.

Таблица 4 – Коэффициенты защищенности

Поток	**Коэффициент**			**Наименьший коэффициент**
	локальной защищенности информации	**удаленной защищенности информации**	**локальной защищенности рабочего места группы**	
Главный бухгалтер/база бухгалтерии	42	—	57	42
Главный администратор/почтовый сервер	—	47	—	47
Администратор файловых серверов/файловый сервер	—	47	—	47
Сетевой администратор/почтовый сервер	—	47	—	47
Сотрудники/система контроля версий	—	47	57	47

При использовании VPN-технологии для обеспечения безопасности ИС, она не учитывается при локальном доступе. В случае удаленного доступа к наименьшему коэффициенту защищенности прибавляется установленный вес VPN-шлюза – 20 *(таблица 5).*

Учтем количество человек в каждой группе *(таблица 6)*. Если к информации имеет доступ группа пользователей, превышающая 50 человек, то это увеличивает

итоговый коэффициент. Если группа пользователей имеет доступ в Интернет, то это увеличивает итоговый коэффициент в два раза.

Таблица 5 — Коэффициенты защищенности с учетом технологии VPN

Поток	**Наименьший коэффициент**	**Вес VPN-соединения**	**Результирующий коэффициент**
Главный бухгалтер/база бухгалтерии	42	—	42
Главный администратор/почтовый сервер	47	20	67
Администратор файловых серверов/файловый сервер	47	20	67
Сетевой администратор/почтовый сервер	47	20	67
Сотрудники/система контроля версий	47	20	67

Таблица 6 — Коэффициенты защищенности с учетом состава групп

Поток	**Результирующий коэффициент**	**Количество человек в группе**	**Наличие у группы доступа в Internet**	**Итоговый коэффициент**
Главный бухгалтер/база бухгалтерии	42	1	1	0,047
Главный администратор/почтовый сервер	67	1	2	0,029
Администратор файловых серверов/файловый сервер	67	1	2	0,029
Сетевой администратор/почтовый сервер	67	1	2	0,029
Сотрудники/система контроля версий	67	136	2	0,405

Для расчета итоговой вероятности необходимо установить базовую вероятность и умножить ее на итоговый коэффициент. Результаты представлены в *таблице 7*.

Таблица 7 — Расчет итоговой вероятности

Поток	**Базовая вероятность**	**Итоговый коэффициент**	**Итоговая вероятность**
Главный бухгалтер/база бухгалтерии	0,7	0,047	0,0329

Главный администратор/почтовый сервер	0,5	0,029	0,015
Администратор файловых серверов/файловый сервер	0,5	0,029	0,015
Сетевой администратор/почтовый сервер	0,5	0,029	0,015
Сотрудники/система контроля версий	0,6	0,405	0,243

Итоговая вероятность для информации, к которой имеют доступ несколько групп пользователей, рассчитывается по формуле $P_{inf} = 1 - \prod_{(P_{ug,n})}(1 - P_{ug,n})$. Результаты представлены в *таблице 8*.

Таблица 8 – Оценка риска по угрозе конфиденциальности

Информация	**Итоговая вероятность**	**Ущерб от реализации угрозы**	**Оценка риска**
База бухгалтерии	0,033	100	3,3
Почтовый сервер	0,031	100	3,1
Файловый сервер	0,015	100	1,5
Система контроля версий	0,243	100	24,3

Рассчитаем риск по угрозе целостности. Коэффициенты защищенности вычисляются аналогично угрозе конфиденциальности. Учтем средства резервирования и контроля целостности *(таблица 9).*

Таблица 9 — Коэффициенты защищенности с учетом применения средств резервирования и контроля целостности

Поток	**Наименьший коэффициент**	**Вес VPN-соединения**	**Веса средств резервирования и контроля целостности**	**Результирующий коэффициент**
Главный бухгалтер/база бухгалтерии	42	—	—	42
Главный администратор/почтовый сервер	47	20	—	67
Администратор файловых	47	20	10	77

серверов/файловый сервер				
Сетевой администратор/почтовый сервер	47	20	—	67
Сотрудники/система контроля версий	47	20	10	77

Учтем наличие в КИС резервного канала, количество человек в группе пользователей и наличие у группы пользователей доступа в сеть Интернет *(табл. 10)*. Расчет итоговой вероятности представлен в *таблице 11*.

Таблица 10 – Коэффициенты защищенности с учетом количества человек в группе и наличия доступа в сеть Интернет

Поток	**Результирующий коэффициент**	**Количество человек в группе**	**Наличие у группы доступа в Internet**	**Итоговый коэффициент**
Главный бухгалтер/база бухгалтерии	42	1	1	0,023
Главный администратор/почтовый сервер	67	1	2	0,029
Администратор файловых серверов/файловый сервер	77	1	2	0,025
Сетевой администратор/почтовый сервер	67	1	2	0,029
Сотрудники/система контроля версий	77	136	2	0,353

Таблица 11 — Расчет итоговой вероятности

Поток	**Базовая вероятность**	**Итоговый коэффициент**	**Итоговая вероятность**
Главный бухгалтер/база бухгалтерии	0,7	0,023	0,016
Главный администратор/почтовый сервер	0,5	0,029	0,015
Администратор файловых серверов/файловый сервер	0,5	0,025	0,013

Сетевой администратор/почтовый сервер	0,5	0,029	0,015
Сотрудники/система контроля версий	0,6	0,353	0,212

При расчете рисков по угрозе доступности проанализируем средства резервирования: резервный канал.

Влияние резервного канала учитывается в том случае, если группа обычных пользователей (не Интернет-пользователей) имеет только удаленный доступ к информации на ресурсе. Наличие доступа в сеть Интернет учтено в *таблице 12*. Итоговое время простоя представлено в *таблице 13*.

Таблица 12 – Итоговые коэффициенты защищенности

Поток	**Коэффициент защищенности**	**Наличие у группы доступа в Internet**	**Итоговый коэффициент**
Главный бухгалтер/база бухгалтерии	2	1	2
Главный администратор/почтовый сервер	1	2	2
Администратор файловых серверов/файловый сервер	1	2	2
Сетевой администратор/почтовый сервер	1	2	2
Сотрудники/система контроля версий	2	2	4

Таблица 13 – Итоговое время простоя

Поток	**Базовое время простоя**	**Итоговое базовое время простоя**	**Итоговый коэффициент**	**Промежуточное время простоя**	**Итоговое время простоя**
Главный бухгалтер/ база бухгалтерии	70	70	2	140	140
Главный администратор/ почтовый сервер	50	70	2	140	140
Администратор файловых серверов/файловый сервер	50	50	2	100	100

Поток	Базовое время простоя	Итоговое базовое время простоя	Итоговый коэффициент	Промежуточное время простоя	Итоговое время простоя
Сетевой администратор/почтовый сервер	50	60	2	120	120
Сотрудники/система контроля версий	60	70	4	280	280

Оценка рисков по угрозе доступности приведена в *таблице 14*.

Таблица 14 – Риски по угрозе доступности

Информация	Итоговое время простоя	Ущерб от реализации	Оценка риска
База бухгалтерии	140	1	140
Почтовый сервер	130	1	130
Файловый сервер	100	1	100
Система контроля версий	280	1	280

Для примера использования модели угроз/уязвимостей рассмотрим информационный ресурс, представленный рабочей станцией бухгалтера с базой данных бухгалтерии.

Для данного ресурса применимы следующие угрозы:

- Физические внешние угрозы: удар молнии, отключение электроснабжения.
- Физическое воздействие нарушителя: проникновение внутрь охраняемого периметра и кража носителя информации;
- Программные угрозы: запуск файла, содержащего компьютерный вирус.

Угрозы могут быть реализованы через следующие уязвимости:

1) отсутствует система резервирования;
2) не используется автоматическая защита электрооборудования;
3) не производится регулярное обновление антивирусных баз;
4) допущены типовые ошибки при настройке операционной системы.

Определим для каждой пары «угроза-уязвимость» вероятность и критичность реализации угрозы методом экспертных оценок и построим *таблицу 15* соответствия угроз/уязвимостей.

Таблица 15 – Оценка критичности реализации угроз

Угроза	**Уязвимости**	**Вероятность реализации угрозы в течение года, %**	**Критичность реализации угрозы, %**
Удар молнии	Отсутствует система резервирования	5	70
	Не используется автоматическая защита электрооборудования	5	70
Отключение электроснабжения	Отсутствует система резервирования	60	70
	Не используется автоматическая защита электрооборудования	40	70
Запуск файла, содержащего компьютерный вирус	Не производится регулярное обновление антивирусных баз	30	60
	Допущены типовые ошибки при настройке операционной системы	15	60

Рассчитаем риск реализации угроз через уязвимости и определим риск реализации каждой угрозы *(таблица 16)*.

Рассчитаем риск безопасности ресурса по формуле:

$R(K, R_i) = K(1 - \prod_{i=1}^{m}(1 - R_i))$, где m – количество угроз, K – критичность ресурса. Возьмем критичность ресурса равную 50%.

$R(K, R_i) = 0{,}36$

Таблица 16 – Определения риска реализации угрозы

Угроза	**Уязвимости**	$\mathbf{R_{i,j}}$	$\mathbf{R_i}$
Удар молнии	Отсутствует система резервирования	0,04	0,08
	Не используется автоматическая защита электрооборудования	0,04	

Отключение электроснабжения	Отсутствует система резервирования	0,42	0,58
	Не используется автоматическая защита электрооборудования	0,28	
Запуск файла, содержащего компьютерный вирус	Не производится регулярное обновление антивирусных баз	0,18	0,25
	Допущены типовые ошибки при настройке операционной системы	0,09	

Контрольные вопросы

1. Какой подход к анализу КИС используют в модели информационных потоков?

Анализ аспектов и факторов защищенности ИС, ее архитектуры и среды эксплуатации.

2. Перечислите данные об ИС, необходимые для построения модели информационных потоков?

Необходимые для построения модели информационных потоков ИС данные:

- деление ценной информации на виды;
- знание величины ущерба для каждого вида ценной информации по трем видам ущерба;
- перечень всех ресурсов, на которых хранится информация;
- средства защиты информации;
- средства защиты рабочих мест групп пользователей.

3. Относительно каких взаимодействующих элементов КИС рассчитывают риски в модели информационных потоков?

Риск оценивается отдельно по каждой связке «группа пользователей — информация», т.е. модель рассматривает взаимосвязь «субъект — объект», учитывая все их характеристики.

4. Укажите коэффициенты, используемые в модели информационных потоков при расчете уровня риска.

Коэффициенты:

- локальной защищенности информации на ресурсе;
- удаленной защищенности информации на ресурсе;
- локальной защищенности рабочего места группы пользователей.

5. В каких единицах измеряется ущерб от угрозы доступности при расчете риска с помощью модели информационных потоков?

В часах.

6. Какие компоненты КИС рассматриваются в модели угроз/уязвимостей?

Уязвимость, угроза, ресурс.

7. Как соотносятся угрозы безопасности и уязвимости ресурсов?

Свойством угрозы безопасности является перечень уязвимостей, при помощи которых угроза может быть реализована.

8. Чем отличается критичность реализации угрозы от критичности ресурса?

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс; критичности ресурса – степень значимости ресурса для КИС, то есть насколько сильно реализация угроз безопасности, направленных на ресурс, повлияет на работу всей КИС.

9. Укажите способы определения угроз нарушения безопасности, которым подвержен ресурс КИС.

Способы определения угроз безопасности:

- определяются возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности информации;
- определяются уязвимости, которые могут использоваться при реализации угроз безопасности информации (включая специально внедренные программные закладки);
- определяются способы (методы) реализации угроз безопасности информации;
- определяются объекты информационной системы, на которые направлена угроза безопасности информации (объекты воздействия).

10. Предложите формулу расчета риска по угрозе доступности ресурса.

При расчете рисков по угрозе доступности базовые времена простоя наследуются только в пределах ресурса. Для информации, к которой имеет доступ несколько групп пользователей, итоговое время простоя рассчитывается по формуле:

$$T_{inf} = \left(1 - \prod_{(T_{ug,n})} (1 - \frac{T_{ug,n}}{T_{max}})\right) T_{max}$$

Вывод

В ходе данной лабораторной работы был изучен метод декомпозиции активов систем на компоненты информационных взаимодействий, получены навыки анализа защищенности ресурсов и численной оценки рисков с помощью модели информационных потоков и модели угроз/уязвимостей. Построенные модель позволили рассчитать риски нарушения безопасности информации по угрозам конфиденциальности, целостности и доступности, с использованием опыта экспертной оценки обрабатываемой и хранимой в ИС информации.