МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУГРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ им. проф. М.А. БОНЧ-БРУЕВИЧА»

Факультет Информационных систем и технологий
Кафедра Информационных управляющих систем

РАБОТА
ЗАЩИЩЕНА С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

проф., д.т.н.		Н.Н. Мошак
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ПРАКТИЧЕСКАЯ РАБОТА № 2

«Оценка риска информационной безопасности корпоративной информационной системы на основе модели информационных потоков»

по курсу: Защищенные информационные системы

РАБОТУ ВЫПОЛНИЛ(А)
СТУДЕНТ(КА) ГР. _____ _____ _____
подпись, дата инициалы, фамилия

Санкт-Петербург 2017

Цель работы: рассчитать риск информационной безопасности корпоративной информационной системы на основе модели информационных потоков

1. Постановка задачи

Современные ИС строятся, как правило, на архитектуре «клиент-сервер» с применением технологии виртуальных серверов и предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищенности, обрабатывается конфиденциальная информация с различным грифом секретности, а в «открытом» контуре - открытая информация. При этом сертифицированными средствами однонаправленной передачи информации обеспечивается только односторонняя передача информации из «открытого» контура в «закрытый». Типовая схема организации взаимодействия контуров ИС СН приведена на рис.1.

Вешнее взаимодействие ИС с корпоративными системами осуществляется через «закрытый» контур с применением сертифицированных средств криптографической защиты информации (СКЗИ) с шифрованием информации, а с другими системами – через «открытый» контур с применением сертифицированных межсетевых экранов (МЭ).

В качестве базового сетевого протокола используется IP-протокол.

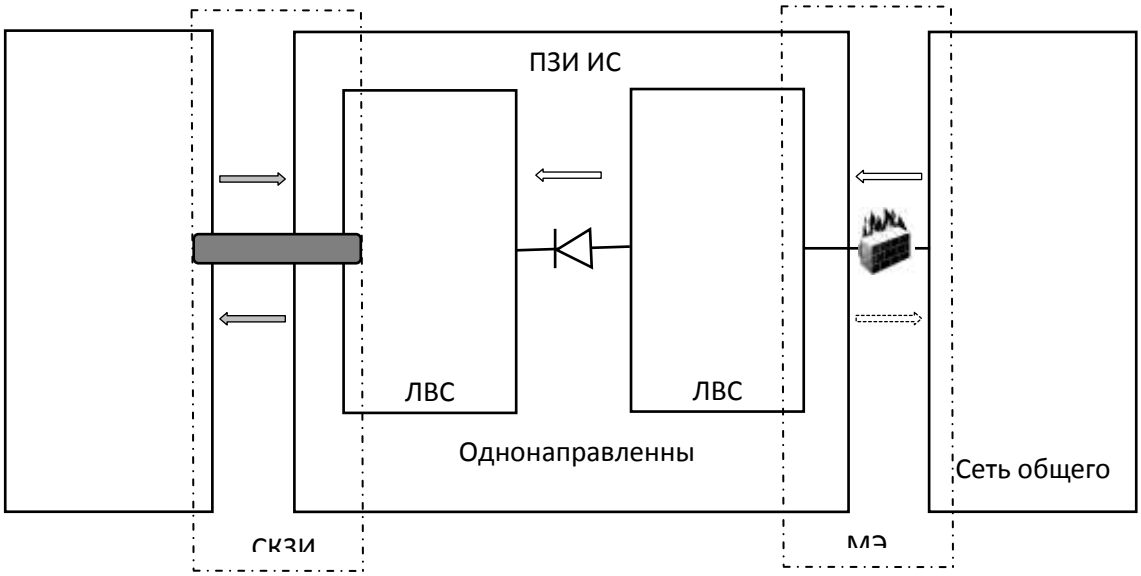

Рис. 1 - Общая схема взаимодействия «закрытого» и «открытого» контуров предприятия

В общем случае корпоративная ИС организации на технологии «клиент-сервер» включает в себя следующие функциональные компоненты:

- сервера СУБД и файл-сервера, осуществляющие обработку и хранение инфоуслуг;
- автоматизированные рабочие места (АРМ) – оконечные абонентские системы ИС;

• корпоративная мультисервисная сеть связи на основе IP-QoS технологий, включающая в себя локальную вычислительную сеть (ЛВС) и WAN-компоненту, обеспечивающую связь территориально удаленных ЛВС организации. В корпоративную сеть входят структурированные кабельные системы (СКС), на базе которых строятся ЛВС предприятия, сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.) и внешние каналы связи. а также механизмы, обеспечивающие их функционирование, в том числе системы и средства защиты информации.

Анализ информационных рисков позволяет эффективно управлять информационной безопасностью автоматизированной системой обработки информации (АСОИ) или корпоративной информационной системой (КИС) предприятия (организации). Для этого в начале работ по анализу рисков необходимо определить, что именно подлежит защите на предприятии и воздействию каких угроз оно подвержено, а затем выработать рекомендации по практике защиты. Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Анализ риска можно проводить согласно методике по сценарию, представленному на рис. 2. Каждый из шести этапов анализа риска должен быть конкретизирован.

На первом и втором этапах выявляются сведения, составляющие для предприятия коммерческую тайну, которые предстоит защищать.

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия.

В связи с этим необходимо еще раз подчеркнуть, что степень информационной безопасности определяется не только (а может быть и не столько) средствами и способами защиты, но и особенностями построения КИС. И когда говорят о **КИС в защищенном исполнении, речь идет прежде всего о выборе такой архитектуры (топологии) системы обработки информации, расположения средств обработки конфиденциальной информации и способов ее хранения и передачи, которые существенно уменьшат число возможных точек доступа к информации.**

Третий этап анализа риска - построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС.

Рис.2 Общая схема взаимодействия «закрытого» и «открытого» контуров предприятия - Сценарий анализа информационных рисков компании

Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

Анализ способов защиты всех возможных точек атак соответствует целям защиты, и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств (четвертый этап).

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей находятся вероятности реализации угроз по каждой из возможных точек атак.

На заключительном этапе производится оценка ущерба организации в случае реализации каждой из атак. Эти данные вместе с оценками уязвимости позволяют получить ранжированный список угроз информационным ресурсам.

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу - это произведение вероятности нападения на ресурс, вероятности реализации угрозы и ущерба от информационного вторжения. В данном произведении могут быть использованы различные способы взвешивания составляющих.

Объединение рисков по всем ресурсам дает общую величину риска при принятой архитектуре КИС и внедренной в нее системы защиты информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, можно (за счет изменения вероятности реализации угроз) представить и рассмотреть различные значения риска. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с заданным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности так-же нужно определить **стратегию управления рисками** на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных - *уменьшение риска путем принятия комплексной системы контрмер*, включающей программно-технические и организационные меры защиты. Близким является подход, связанный *с уклонением от риска*. От некоторых классов рисков можно уклониться, например: вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее - бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

После того как стратегия управления рисками выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

Отметим, что выполнение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих областях, смежных с проблемой защиты информации.

2. Методы оценивания информационных рисков

В настоящее время используются различные методы оценки информационных рисков отечественных компаний и управления ими. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

1) идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;
2) оценивание возможных угроз;
3) оценивание существующих уязвимостей;
4) оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы. При этом информационные риски компании зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается

вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

– привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);

– возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);

– техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;

– степенью легкости, с которой уязвимость может быть использована.

3. Основные понятия и допущения модели

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Критичность ресурса **(D) –** ущерб, который понесет компания от потери ресурса. Задается в уровнях (количество уровней может быть в диапазоне от 2 до или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (Dc, Di, Da).

4. Метод оценки рисков на основе модели информационных потоков (*"Методика оценки рисков информационной безопасности компании Digital Security"*)

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Данная модель позволяет оценить защищенность каждого вида информации.

Алгоритм позволяет получить следующие данные:

- Реестр ресурсов;
- Значения риска для каждого ценного ресурса организации;
- Значения риска для ресурсов после задания контрмер (остаточный риск);
- Эффективность контрмер;
- Рекомендации экспертов.

Для того, чтобы построить модель ИС, необходимо проанализировать защищенность и архитектуру построения информационной системы.

Специалист по ИБ, привлекая владельца (менеджера) информационной системы (используя вопросники, интервью, документацию, инструменты автоматического сканирования), должен подробно ***описать архитектуру сети:***

• все аппаратные (компьютерные) ресурсы, на которых хранится ценная информация;

• сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);

- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз;
- бизнес-процессы, в которых обрабатывается информация;
- пользователей (группы пользователей), имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности **каждого вида информации** на ресурсе.

Целесообразно составить карту ИС на которой отобразить все указанные характеристики. Иными словами, необходимо:

4.1. Изобразить ИС в виде структурной схемы, на которой отобразить:

- все ресурсы (сервер, АРМ и т.д.);
- отделы, к которым относятся ресурсы;
- сетевые группы (локальные сети), физические связи ресурсов между собой и их подключения к Интернет;
- виды ценной информации, хранящейся на ресурсах;
- пользователей (группы пользователей), имеющих доступ к ценной (конфиденциальной) информации.

Пример структурной схемы ИС приведен на рис.3.

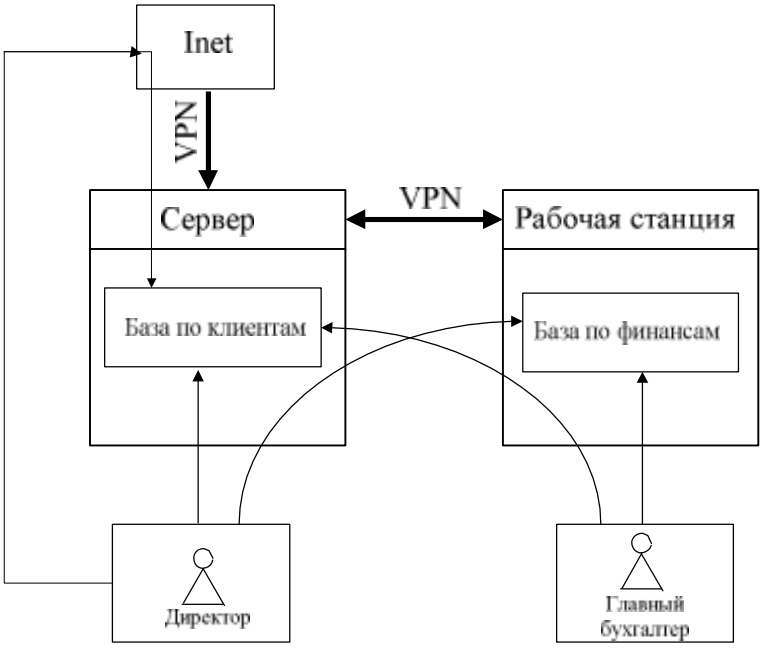

Рис. 3 - Структурная схема ИС

4.2. Описать в виде таблиц средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящемся на нем с указанием веса каждого средства, например:

Средства защиты сервера	Вес
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помеще- ние)	25
Средства локальной защиты	
Отсутствие дисководов и USB портов 10	10
Средства корпоративной сетевой защиты	
Межсетевой экран	10
Обманная система	2
Система антивирусной защиты на сервере	10
Средства резервирования и контроля целостности	
Аппаратная система контроля целостности	20
Средства защиты информации (информация №1)	Вес
Средства локальной защиты	
Средства криптографической защиты (криптозащита данных на ПК)	20
Средства резервирования и контроля целостности	
Резервное копирование	10
Программная система контроля целостности	10

Средства защиты рабочей станции	Вес
Средство физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение)	10
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	10
Средства персональной сетевой защиты	
Наличие персонального межсетевого экрана	3
Система криптозащиты электронной почты	10

4.3. Описать в виде таблицы вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а так же наличие соединения через VPN, количество человек в группе для каж- дого информационного потока:

Информационный поток	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
(Наименование)	(Локальный, удаленный)	(Чтение, запись, удаление)	(Да, нет)	(1,2,….n)

4.4. Указать наличие у пользователей выхода в Интернет

Пользователь (группа пользователей.)	Доступ в Интернет
(Наименование)	(Есть, нет, не анализируется)

4.5. Указать ущерб компании от реализации угроз ИБ для каждого информационного потока:

Информационный поток	Конфиденциальность	Целостность	Доступность
(Наименование)	(у.е. в год)	(у.е. в год)	(у.е. в час)

Ущерб определяется с участием владельца ИС, либо им самим непосредственно. На этом описание архитектуры ИС завершается.

Далее производится расчет рисков **для каждого вида ценной информации хранящейся в ИС** по угрозе «нарушение конфиденциальности».

5. Расчет рисков по угрозе конфиденциальность

5.1. Расчет коэффициентов защищенности.

Для каждого информационного потока рассчитывается коэффициент локальной либо удаленной защищенности информации, хранящейся на ресурсе, в зависимости от типа доступа. Если доступ локальный, то рассчитывается только коэффициент локальной защищенности информации. Если доступ удаленный, то рассчитывается коэффициент удаленной защищенности информации, хранящейся на ресурсе и коэффициент локальной защищенности рабочего места пользователя.

Коэффициент локальной защищенности информации рассчитывается, если доступ к информации в данном информационном потоке ***локальный***. Он равен сумме весов средств физической и локальной защиты информации. Учитываются все средства физической защиты и средства локальной защиты информации, обеспечивающие защиту информации по угрозе ***конфиденциальность***:

- средства физической защиты: охрана, замок, пропускной режим в помещение) (25);
- средства локальной защиты:
- отсутствие дисководов и USB портов (10);
  криптозащита данных на ПК (20).

Коэффициент удаленной защищенности информации на ресурсе рассчитывается, если доступ к информации в данном информационном потоке *удаленный*. Он необходим для того, чтобы учесть сетевые средства защиты, и равен сумме весов средств корпоративной сетевой защиты информации. Эти средства (межсетевой экран, серверная антивирусная защита) находятся **на сервере.**

Коэффициент локальной защищенности рабочего места пользователя (группы пользователей) рассчитывается только при удаленном доступе к информации. Он равен сумме весов средств ***физической, локальной*** и ***персональной сетевой защиты*** информации.

Средства физической защиты – те же.

Средства локальной защиты: антивирус, отсутствие дисководов и USB-портов.

Средства персональной сетевой защиты: межсетевой экран (брандмауэр), средства криптозащиты электронной почты.

Эти средства (персональный межсетевой экран – брандмауэр, средства криптозащиты электронной почты) находятся на рабочей станции (на компьютере, подключенном к локальной сети).

Этот коэффициент не определяется для анонимных и авторизованных Интернет-пользователей, т.к. рабочее место пользователя в данном случае не является частью ИС.

Для дальнейших расчетов по каждому потоку из трех коэффициентов выбирается ***наименьший коэффициент защищенности*** **(НК).**

Информационный поток	*Коэффициент локальной защищенности информации*	*Коэффициент удаленной защищенности информации*	*Коэффициент локальной защищенности рабочего места*	Наименьший коэффициент
(Наименование)	*(Ф+Л)*	*(СКСЗ)*	*(Ф+Л+ПСЗ)*	(НК) min

5.2. Учет наличия доступа при помощи VPN

При локальном доступе VPN не учитывается, поскольку локальная сеть не используется для передачи информации.

При удаленном доступе через VPN к наименьшему коэффициенту защищенности потока прибавляется вес VPN шлюза (20). Это сетевое устройство повышает защищенность информации.

При этом от наименьшего коэффициента переходят к результирующему**: РК=НК+20 (или +0)**

Информационный поток	Наименьший коэффициент	Вес VPN соединения	Результирующий коэффициент
(Наименование)	(НК)	(20 либо 0)	(РК)

5.3. Далее от результирующего коэффициента (РК) переходят к итоговому коэффициенту (ИК) защищенности

Если количество пользователей 1, и у группы нет доступа в Интернет, то: **ИК=1/РК.**

Учет количества человек **N** в группе пользователей: **ИК=N/РК.**

Если группа пользователей имеет доступ в Интернет, то ИК увеличивается в 2 раза:

ИК=2 N/РК.

Если при удаленном доступе Интернет-пользователей VPN-соединение не используется (Интернет заведен на компьютер, а не на сервер), то для них ***итоговый*** коэффициент защищенности (**ИК**) умножается на 4, ***в силу отсутствия зашиты шлюза*** **ИК=(4 N)/РК**

Информационный поток	Результирующий коэффициент	Количество человек в гр.	Наличие Интернет	Итоговый коэффициент
Главный бухгалтер – бухгалтерский	(РК)	(N)	I=2,1	ИК=(N I)/РК

Результаты расчетов сводятся в таблицу.

5.4. Расчет итоговой вероятности (ИВ)

Чтобы получить **ИВ**, необходимо сначала определить **базовую вероятность (БВ)** реализации угрозы нарушения конфиденциальности и умножить ее на **ИК:**

ИВ=БВ·ИК.

БВ реализации угрозы «К» определяется на основе метода экспертных оценок. Группа экспертов определяет БВ для каждой информации (для каждого потока). БВ может задать владелец информации.

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность (ПВ)	Итоговая вероятность (ИВ)
Главный бух-	0,2	0,5	0,036	0,018	0,018

галтер – бухгалтерский отчет					
Бухгалтер – база клиентов Компании	0,2	0,5	0,024	0,012	0,024
Финансовый директор- база клиентов Компании	0,5	0,5	0,024	0,012	
Бухгалтер-база данных наименований товаров Компании	0,2	0,5	0,033	0,0165	0,0165

Итоговая базовая вероятность (**ИБВ**) одинакова для всех потоков, по- скольку к информации «база клиентов Компании» имеется доступ через Интер- нет (Финансовый директор имеет права «запись, чтение»). Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор – база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сете- вую группу).

Это так называемое **наследование коэффициентов защищенности**. Если на ресурсе расположены несколько видов информации, причем к некоторым из них осуществляется доступ через Интернет (группами анонимных, авторизованных или мобильных Интернет-пользователей), то угрозы, исходящие от этих групп пользователей могут повлиять и на другие виды информации. Следовательно, это необходимо учесть. Если на одном из ресурсов, находящемся в сетевой группе, хранится информация, к которой осуществляют доступ указанные группы пользователей, то это учитывается аналогично для всех видов информации, хранящихся на всех ресурсах, входящих в сетевую группу. В реальной информационной системе все ресурсы, взаимосвязанные между собой, оказывают друг на друга влияние. Т.е. злоумышленник, проникнув на один ресурс информационной системы (например, получив доступ к информации ресурса), может без труда получить доступ к ресурсам, физически связанным со взломанным.

Промежуточная вероятность (**ПВ**) вычисляется, как:**ПВ=ИБВ·ИК.**

Итоговая вероятность **ИВ1=ПВ1**; **ИВ3=ПВ3**.

Итоговая вероятность **ИВ2=1-(1-ПВ21) (1-ПВ22)**, как суммарная по двум группам пользователей.

5.5. Расчет риска по угрозе конфиденциальность для каждой информации (1,2,3)

Риск по угрозе конфиденциальность для каждой информации (1-бух. отчет, 2-база клиентов, 3-база наименований товаров) рассчитывается, как произведение итоговой вероятности на ущерб:

R1=ИВ1*D1=0,018*100=1,8;
R2=ИВ2*D2=0,024*100=2,4;
R3=ИВ3*D3=0,0165*100=1,65.

где **У**–ущерб от реализации угрозы.

5.6. Расчет риска по угрозе конфиденциальность для ресурса

Риск для ресурса, на котором хранится несколько видов информаций (несколько БД) равен сумме рисков по всем видам информации.

6. Расчет рисков по угрозе целостность

6.1.Расчет коэффициентов защищенности.

Выполняется аналогично расчету по угрозе конфиденциальность. Фактически берутся наименьшие коэффициенты НК из предыдущего расчета.

6.2.Учет средств резервирования и контроля целостности.

Информационный поток	Наименьший коэффициент (НК)	Вес VPN-соединения	Веса средств резервирования и контроля целостности	Результирующий коэффициент (РК)
Главный бухгалтер – бухгалтерский отчет	55	-	40 АСКЦ-20 РК-10 ЦП-10	95 55+40
Бухгалтер – база клиентов Компании	22	20	20 РК-10 ЦП-10	62 22+20+20
Финансовый директор- - база клиентов Компании	22	20	20 АСКЦ-20	62 22+20+20
Бухгалтер-база данных наименований товаров Компании	30	-	20 РК-10 ЦП-10	50 30+20

6.3. Учет резервного копирования, количества человек в группе пользователей и наличия у группы пользователей доступа в Интернет

Информационный поток	Результирующий коэффициент (РК)	Наличие резервного копирования	Кол-во человек в группе	Наличие у группы доступа в Интернет	Итоговый коэффициент (ИК)
Главный бухгалтер –	95	1	1	2	0,021

бухгалтерский отчет					(1/95)*2
Бухгалтер – база клиентов Компании	62	1	1	1	0,016 1/62
Финансовый директор- - база клиентов Компании	62	4	1	-	0,065 (1/62)*4
Бухгалтер-база данных наименований товаров Компании	50	1	1	1	0,02 1/50

Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес резервного копирования (10) прибавляется к коэффициенту защищенности (п.2). Если резервное копирование не осуществляется, и в группе пользователей, имеющей доступ к информации, разрешены **запись** или **удаление**, то итоговый коэффициент увеличивается в 4 раза.

6.4. Расчет итоговой вероятности

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность	**Итоговая вероятность**
Главный бухгалтер – бухгалтерский отчет	0,25	0,7	0,021	0,0147 0,7*0,021	**0,0147**
Бухгалтер – база клиентов Компании	0,1	0,7	0,016	0,0112 0,7*0,016	**0,05619**
Финансовый директор- - база клиентов Компании	0,7	0,7	0,065	0,0455 0,7*0,065	
Бухгалтер-					

база данных наименова-ний товаров Компании	0,25	0,7	0,02	0,014 0,7*0,02	**0,014**

Базовая вероятность определяется на основе метода экспертных оценок. Ее значения по данной угрозе **целостность** отличаются от значений в расчете по угрозе **конфиденциальность.** Группа экспертов, исходя из классов групп пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец информационной системы, при желании, может задать этот параметр самостоятельно.

Итоговая базовая вероятность. Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор-база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сетевую группу).

Перемножив итоговую базовую вероятность и итоговый коэффициент защищенности, получим итоговую вероятность реализации угрозы. Напомним, что для каждой из трех угроз информационной безопасности мы отдельно рассчитываем вероятность реализации.

Итоговая вероятность по второй информации:

ИВ2=1-(1-ПВ21)*(1-ПВ22), как суммарная по двум группам пользователей.

7. Расчет риска по угрозе целостность

На завершающем этапе значение полученной итоговой вероятности умножаем на ущерб от реализации угрозы и получаем риск угрозы информационной безопасности для связи <вид информации - группа пользователей>.

R1=ИВ1*D1=0,0147*100=1,47;

R2=ИВ2*D2=0,05619*100=5,61; R3=ИВ3*D3=0,014*100=1,4.

Чтобы получить риск для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), необходимо сначала просуммировать итоговые вероятности реализации угрозы по следующей формуле:

$$P_{inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}),$$

а затем полученную итоговую вероятность для информации умножаем на ущерб от реализации угрозы, получая, таким образом, риск от реализации угрозы для данной информации.

Чтобы получить риск для аппаратного ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

ЗАДАНИЕ

Составить карту ИС (см. рис 1) на которой отобразить все указанные характеристики. Иными словами, необходимо

1. Изобразить ИС в виде структурной схемы, на которой отобразить:

- все ресурсы (сервер закрытого контура, сервер открытого контура, МЭ открытого контура, СКЗИ закрытого контура, однонаправленный шлюз, оборудование ЛВС закрытого контура, оборудование ЛВС открытого контура)
- отделы, к которым относятся ресурсы;
- сетевые группы (локальные сети), физические связи ресурсов между собой и их подключения к Интернет;
- виды ценной информации, хранящейся на ресурсах;
- пользователей (группы пользователей), имеющих доступ к ценной (конфиденциальной) информации.

2. ***Описать в виде таблиц средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящемся на нем с указанием веса каждого средства, например:***

Средства защиты сервера	Вес
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	
Средства локальной защиты	
Отсутствие дисководов и USB портов 10	
Средства корпоративной сетевой защиты	
Межсетевой экран	
Обманная система	
Система антивирусной защиты на сервере	
Средства резервирования и контроля целостности	
Аппаратная система контроля целостности	
Средства защиты информации (информация №1)	Вес
Средства локальной защиты	
Средства криптографической защиты (криптозащита данных на ПК)	
Средства резервирования и контроля целостности	
Резервное копирование	
Программная система контроля целостности	

Средства защиты рабочей станции	Вес
Средство физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение)	
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	
Отсутствие дисководов и USB портов	
Средства персональной сетевой защиты	

Наличие персонального межсетевого экрана	
Система криптозащиты электронной почты	

3.Описать в виде таблицы вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а так же наличие соединения через VPN, количество человек в группе для каж- дого информационного потока:

Информационный поток	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
(Наименование)	(Локальный, удаленный)	(Чтение, запись, удаление)	(Да, нет)	(1,2,….n)

4.Указать наличие у пользователей выхода в Интернет

Пользователь (группа пользователей.)	Доступ в Интернет
(Наименование)	(Есть, нет, не анализируется)

5.Указать ущерб компании от реализации угроз ИБ для каждого информационного потока:

Информационный поток	Конфиденциальность	Целостность	Доступность
(Наименование)	(у.е. в год)	(у.е. в год)	(у.е. в час)

Ущерб определяется с участием владельца ИС, либо им самим непосредственно.

На этом описание архитектуры ИС завершается.

Далее производится расчет рисков **для каждого вида ценной информации хранящейся в ИС** по угрозе «нарушение конфиденциальности», «нарушение целостности» и «нарушение доступновсти» по методике, изложенной выше.

P.S. Веса выбирать самостоятельно

Д.т.н., профессор Н.Н.Мошак