Цель работы:

Рассчитать риск информационной безопасности корпоративной информационной системы на основе модели информационных потоков.

Теоретические положения:

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.

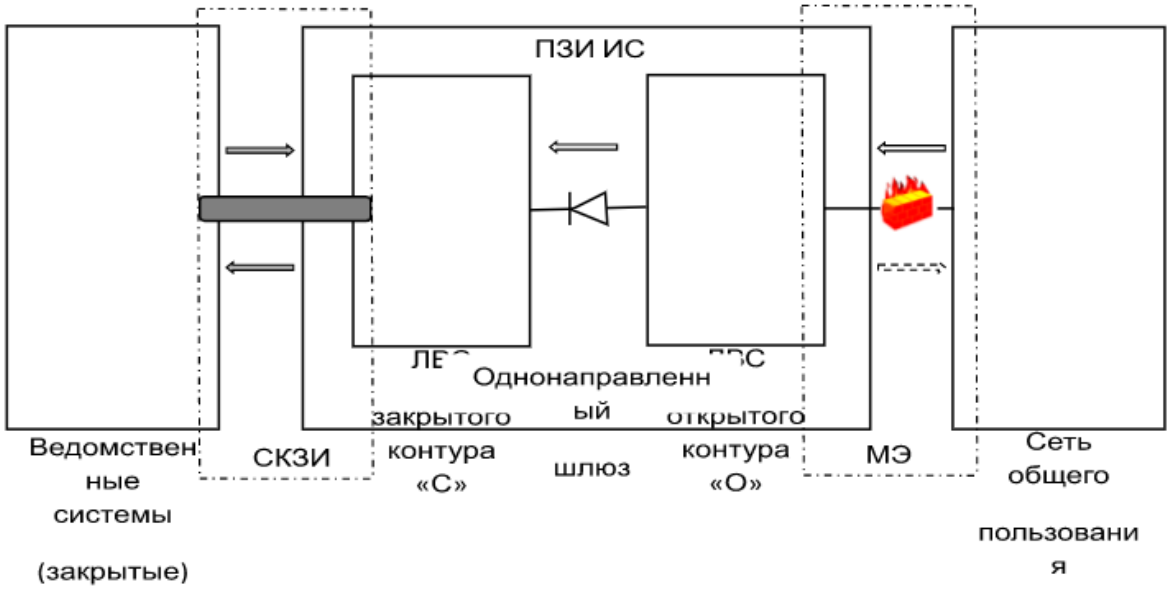

Рис. 1 - Общая схема взаимодействия «закрытого» и «открытого» контуров предприятия

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.

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.

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).

Задание к практической работ оценка рисков ИС на основе модели информационных потоков ("Методика оценки рисков информационной безопасности компании Digital Security")

Построение модели ИС организации

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.

Ход выполнения работы:

В качестве ИС была взята часть отдела автоматизированных систем, которая связана с работой Личного кабинета ГУАП. В качестве ресурсов представлены – сервер и автоматизированное рабочее место (АРМ). В качестве ценной информации – база данных работников со всеми персональными данными, а также исходный код Личного кабинета ГУАП. Исходный код Личного кабинета так же является ценной информацией, потому что если должным образом не защищать его, то могут возникнуть проблемы, когда через него злоумышленник может получить доступ к базе данных работников. База данных работников относится к отделу обработки ПДн, в котором есть начальник отдела. А доступ к исходному коду есть у всех сотрудников отдела АИС, которые отвечают за программирование – программисты.

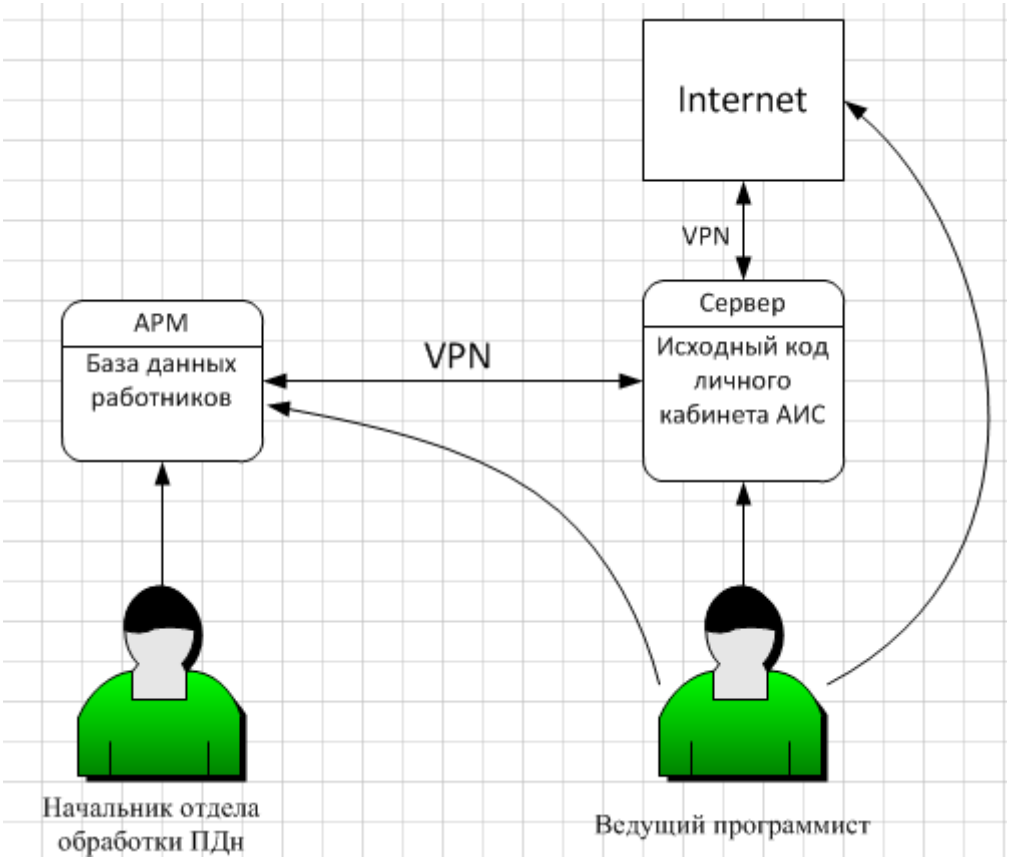

Рисунок 1. Схема ИС.

Средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящемся на нем с указанием веса каждого средства.

Средства защиты сервера	Вес
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещение)	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 АРМ	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

Таблица, в которой должны быть указаны: вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а также наличие соединения через VPN, количество человек в группе для каждого информационного потока.

Информационный поток	**Вид доступа**	**Права доступа**	**Наличие VPN-соединения**	**Количество человек в группе**
Начальник ОО ПДн – база данных работников	Локальный	Чтение, запись, удаление	Нет	1
Ведущий программист – исходный код ЛК АИС	Локальный	Чтение, запись, удаление	Да	4
Ведущий программист – база данных работников	Локальный	Чтение	Да	2

Наличие у пользователей выхода в Интернет

Пояснение: для начальника ПДн выход в Интернет невозможен с компьютера, на котором хранится база данных ПДн работников.

Пользователь (группа пользователей)	**Доступ в Интернет**
Начальник ОО ПДн	Нет
Ведущий программист	Есть

Ущерб организации от реализации угроз ИБ для каждого информационного потока:

Информационный поток	Конфиденциальность (у.е. в год)	Целостность (у.е. в год)	Доступность (у.е. в час)
Начальник ОО ПДн – база данных работников	40	50	20
Ведущий программист – исходный код ЛК АИС	50	60	60
Ведущий программист – база данных работников	60	70	30

Расчет рисков по угрозе конфиденциальность

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

Начальник ОО ПДн – база данных работников	10+10+10			30
Ведущий программист – исходный код ЛК АИС	25+10			35
Ведущий программист – база данных работников	10+10+10			30

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
Начальник ОО ПДн – база данных работников	30	0	30
Ведущий программист – исходный код ЛК АИС	35	20	55
Ведущий программист – база данных работников	30	20	50

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 (РК)	Количество человек в гр. (N)	Наличие Интернет (I)	Итоговый коэффициент (ИК=N*I/РК)

Начальник ОО ПДн – база данных работников	30	1	1	0,033
Ведущий программист – исходный код ЛК АИС	55	2	2	0,073
Ведущий программист – база данных работников	50	4	2	0,12

Чтобы получить **ИВ – итоговую вероятность**, 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)
Начальник ОО ПДн – база данных работников	0,2	0,5	0,033	0,0165	0,07551
Ведущий программист – исходный код ЛК АИС	0,2	0,5	0,073	0,0365	0,0365
Ведущий программист – база данных работников	0,5	0,5	0,12	0,06	0,07551

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.

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

Риск по угрозе конфиденциальность для каждой информации (1-БД работников, 2-база исходный код ЛК АИС) рассчитывается, как произведение итоговой вероятности на ущерб:

R1=ИВ1*D1=0,07551*100=7,551

R2=ИВ2*D2=0,0365*50=1,825

Расчет рисков по угрозе целостность

Информационный поток	*Коэффициент локальной защищенности информации (Ф+Л)*	*Коэффициент удаленной защищенности информации (СКСЗ)*	*Коэффициент локальной защищенности и рабочего места (Ф+Л+ПСЗ)*	Наименьший коэффициент (НК) min
Начальник ОО ПДн – база данных работников	10+10+10			30
Ведущий программист – исходный код ЛК АИС	25+10			35
Ведущий программист – база данных работников	10+10+10			30

Учет средств резервирования и контроля целостности

Информационный поток	Наименьший коэффициент (НК)	Вес VPN-соединения	Веса средств резервирования и контроля целостности	Результирующий коэффициент (РК)
Начальник ОО ПДн – база данных работников	30	0	30 (АСКЦ-20, РК-10)	60 (30+30)
Ведущий программист – исходный код ЛК АИС	35	20	20 (РК-10, ЦП-10)	75 (35+20+20)

Ведущий программист – база данных работников	30	20	20 (РК-10, ЦП-10)	70 (30+20+20)

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

Информаци-онный поток	Результирующий коэффициент (РК)	Наличие резервного копирования	Кол-во человек в группе	Наличие доступа в Интернет	Итоговый коэффициент (ИК)
Начальник ОО ПДн – база данных работников	60 (30+30)	1	1	1	0,0167
Ведущий программист – исходный код ЛК АИС	75 (35+20+20)	1	2	2	0,0533
Ведущий программист – база данных работников	70 (30+20+20)	1	4	2	0,1143

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.

Расчет итоговой вероятности.

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность	Итоговая вероятность
Начальник ОО ПДн – база данных работников	0,7	0,7	0,0167	0,01169	0,0908

Ведущий программист – исходный код ЛК АИС	0,1	0,7	0,0533	0,03731	0,03731
Ведущий программист – база данных работников	0,25	0,7	0,1143	0,08001	0,0908

Расчет риска по угрозе целостность

R1=ИВ1*D1=0,0908*120=10,896
R2=ИВ2*D2=0,03731*60=2,386

Расчет рисков по угрозе доступность

Информационный поток	*Коэффициент локальной защищенности информации (Ф+Л)*	*Коэффициент удаленной защищенности информации (СКСЗ)*	*Коэффициент локальной защищенности и рабочего места (Ф+Л+ПСЗ)*	Наименьший коэффициент (НК) min
Начальник ОО ПДн – база данных работников	10+10+10			30
Ведущий программист – исходный код ЛК АИС	25+10			35
Ведущий программист – база данных работников	10+10+10			30

Учет средств предотвращения потери доступности

Информационный поток	Наименьший коэффициент (НК)	Вес VPN-соединения	Веса средств предотвращения потери доступности	Результирующий коэффициент (РК)
Начальник ОО ПДн – база данных работников	30	0	22 (МЭ – 10, ОС – 2, САЗ – 10)	55 (30+22)

Ведущий программист – исходный код ЛК АИС	35	20	13 (ПМЭ-3, СКЭП-10)	68 (35+20+13)
Ведущий программист – база данных работников	30	20	13 (ПМЭ-3, СКЭП-10)	63 (30+20+13)

Учет количества человек в группе пользователей и наличия у группы пользователей доступа в Интернет

Информационный поток	Результирующий коэффициент (РК)	Кол-во человек в группе	Наличие доступа в Интернет	Итоговый коэффициент (ИК)
Начальник ОО ПДн – база данных работников	55	1	1	0,018
Ведущий программист – исходный код ЛК АИС	68	2	2	0,0588
Ведущий программист – база данных работников	63	4	2	0,126

Расчет итоговой вероятности.

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность	Итоговая вероятность
Начальник ОО ПДн – база данных работников	0,6	0,6	0,018	0,0108	0,0855
Ведущий программист – исходный код ЛК АИС	0,4	0,6	0,0588	0,03528	0,03528

Ведущий программист – база данных работников	0,35	0,6	0,126	0,0756	0,0855

Расчет риска по угрозе доступности

R1=ИВ1*D1=0,0855*50=4,275
R2=ИВ2*D2=0,03528*60=2,1168

Выводы:

Данная методика помогает специалисту по информационной безопасности просчитать все риски по угрозам конфиденциальности, доступности и целостности. Очень часто бывает так, что начальство несерьезно относится к рекомендациям специалиста по ИБ, потому что не разбирается в этом. Если предоставить начальнику расчеты с полученными значениями, то эти значения смогут помочь начальству как-то оценить количественно величину риска и будет более внимателен ко всем проводимым мероприятиям, связанным с ИБ. Архитектура информационной системы помогает определить, на каком этапе могла произойти утечка информации и кто понесет ответственность за нарушение одного из свойств ценной информации: конфиденциальности, целостности или доступности.