Содержание:

ВВЕДЕНИЕ

В настоящее время, когда основные бизнес-процессы предприятий организованы в корпоративных сетях, стает актуальной проблема обеспечения бесперебойной работы корпоративной сети и информационных систем предприятия. Руководящим документом по обеспечению информационной безопасности является политика информационной безопасности предприятия.

Целью данной работы является исследование видов и состава угроз информационной безопасности.

Для достижения поставленной цели, необходимо выполнение следующих задач:

1. Провести анализ предметной области;
2. Провести анализ активов организации и отранжировать их;
3. Провести анализ угроз и уязвимостей для каждого актива;
4. Провести анализ программно-технической архитектуры предприятия;
5. Провести анализ существующих технических средств охраны;
6. Разработать перечень решений по правовому, инженерному и организационному обеспечению ИБ;
7. Провести экономическое обоснование проекта ИБ.

Объект исследования – информационная безопасность.

Предмет исследования - виды и состав угроз информационной безопасности.

Структура работы состоит из введения, основной части, заключения и списка литературы.

Теоретической и методологической базой данной работы послужили трудв российских и зарубежных авторов в области информационной безопасности, материалы периодических изданий и сети Интернет

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Идентификация и оценка информационных активов

Обоснование выбора активов: из возможных видов активов выбраны программные, информационные и физические активы. Это обусловлено тем, что в организации используются информационные системы, с многопользовательским режимом доступа.

Из физических активов выбран только сервер информации, так как он является носителем коммерчески важной информации. Неработоспособность сервера влечет простои в работе предприятия и несет убытки.

Из информационных активов ценность представляет информация о текущих сделках предприятия и персональная информация клиентов и сотрудников. Данный факт обусловлен тем, что потеря информации по сделкам влечет приостановление в работе предприятия, затраты на восстановление информации, а потеря клиентской базы влечет потерю клиентов и негативно сказывается на репутации организации.

Перечень информации конфиденциального характера обусловлен конфиденциальностью персональных данных сотрудников и клиентов. Вопросы конфиденциальности персональных данных регламентированы ФЗ «О персональных данных».

Перечень сведений конфиденциального характера приведены в таблице 1.1.

Таблица 1.1

Перечень сведений конфиденциального характера

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, №№ статей

1.	Персональные данные сотрудников	конфиденциально	Федеральный закон Российской Федерации от 27 июля 2016 г. N 152-ФЗ «О персональных данных»
2.	Персональные данные клиентов	конфиденциально	Федеральный закон Российской Федерации от 27 июля 2016 г. N 152-ФЗ «О персональных данных»
3.	Инструкции по безопасности	Строго конфиденциально	Федеральный закон от 29.07.2014 № 98-ФЗ «О коммерческой тайне» Федеральный закон «Об информации, информационных технологиях и о защите информации» Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»
4.	Информация о деятельности предприятия	Строго конфиденциально	Федеральный закон от 29.07.2014 № 98-ФЗ «О коммерческой тайне»

Ранжирование информации осуществляется пропорционально возможному ущербу от утери или разглашения данной информации.

Максимальный ранг имеет информация о деятельности предприятия.

Разглашение инструкции по безопасности или таблицы учетных записей влечет за собой возможное нарушение информационной безопасности организации, поэтому также имеет высокий ранг.

Нарушения работы сервера без потери информации влекут за собой простои в работе предприятия.

Наименьший ранг активов имеют персональные данные сотрудников, так как разглашение данной информации слабо доказуемо, а потеря информации в случае повреждения носителей не влечет штрафных санкций.

Результат ранжирования активов по степени ценности приведен в таблице 1.2.

Таблица 1.2

Результаты ранжирования активов

Наименование актива	**Ценность актива (ранг)**
Инструкции по безопасности (информационный актив)	4
«1С: Предприятие 8.0» (актив программного обеспечения)	4
Информация о деятельности предприятия (информационный актив)	5
Персональные данные клиентов (информационный актив)	4
Персональные данные сотрудников (информационный актив)	3
Сервер БД (физический актив)	3

Оценка уязвимостей - этот вид оценки предполагает идентификацию уязвимостей окружающей среды, организации, процедур, персонала, менеджмента, администрации, аппаратных средств, программного обеспечения или аппаратура связи, которые могли бы быть использованы источником угроз для нанесения ущерба активам и деловой деятельности организации, осуществляемой с их использованием. Само по себе наличие уязвимостей не наносит ущерба, поскольку для этого необходимо наличие соответствующей угрозы. Наличие уязвимости при отсутствии такой угрозы не требует применения защитных мер, но уязвимость

должна быть зафиксирована и в дальнейшем проверена на случай изменения ситуации. Следует отметить, что некорректно использующиеся, а также неправильно функционирующие защитные меры безопасности могут сами по себе стать источниками появления уязвимостей.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива, которые могут использоваться иным образом или для иных целей, чем те, для которых приобретался или изготавливался данный актив.

В процессе оценки уязвимости происходит идентификация уязвимостей, в которых могут быть реализованы возможные угрозы, а также оценка вероятного уровня слабости, т.е. легкости реализации угрозы.

Исходные данные для оценки уязвимости должны быть получены от владельцев или пользователей актива, специалистов по обслуживающим устройствам, экспертов по программным и аппаратным средствам систем информационных технологий.

Важно оценить, насколько велика степень уязвимости или насколько легко ее можно использовать. Степень уязвимости следует оценивать по отношению к каждой угрозе, которая может использовать эту уязвимость в конкретной ситуации.

После завершения оценки уязвимостей должен быть составлен перечень уязвимостей и проведена оценка степени вероятности возможной реализации отмеченных уязвимостей, например «высокая», «средняя» или «низкая».

Оценку уязвимостей в организации осуществляет начальник службы безопасности с периодичностью раз в квартал. Оценка осуществляется внешней компанией, специализирующейся на проектировании систем ИБ.

В таблице 1.3 приведена оценка уязвимостей активов [4]. Оценка и идентификация уязвимостей производилась в соответствие с ГОСТ Р ИСО/МЭК ТО 13335-3-2007.

Таблица 1.3

Оценка уязвимостей активов

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональны данные сотрудник
1. Среда и инфраструктура				
Отсутствие физической защиты зданий, дверей и окон	+	+		
Неправильное или халатное использование физических средств управления доступом в здания, помещения			+	+
Нестабильная работа электросети				
2. Аппаратное обеспечение				
Отсутствие схем периодической замены				
Подверженность колебаниям напряжения				
Подверженность температурным колебаниям				

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональны данные сотрудник
Подверженность воздействию влаги, пыли, загрязнения				
Чувствительность к воздействию электромагнитного излучения				
Недостаточное обслуживание/неправильная инсталляция запоминающих сред				
Отсутствие контроля за эффективным изменением конфигурации				
3. Программное обеспечение				
Отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей	+	+	+	+

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональны данные сотрудник
Отсутствие аудиторской проверки	+	+	+	+
Незащищенные таблицы паролей				
Плохое управление паролями				
Неправильное присвоение прав доступа				
Отсутствие резервных копий	+	+	+	+
4. Коммуникации				
Незащищенные линии связи	+	+	+	+
Отсутствие идентификации и аутентификации отправителя и получателя	+	+	+	+
Незащищенные потоки конфиденциальной информации	+	+	+	+

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональны данные сотрудник
Незащищенные подключения к сетям общего пользования			+	+
5. Документы (документооборот)				
Хранение в незащищенных местах	+	**+**	**+**	**+**
Недостаточная внимательность при уничтожении	+	+	+	+
Бесконтрольное копирование	**+**	**+**	**+**	**+**
6.Персонал				
Отсутствие надзора за работой лиц, приглашенных со стороны, или за работой уборщиц				
Недостаточная подготовка персонала по вопросам обеспечения безопасности	**+**	**+**	**+**	**+**

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональны данные сотрудник
Несоответствующие процедуры набора кадров				
7. Общие уязвимые места				
Отказ системы вследствие отказа одного из элементов				
Неадекватные результаты проведения технического обслуживания				

Угроза (потенциальная возможность неблагоприятного воздействия) обладает способностью наносить ущерб системе информационных технологий и ее активам. Если эта угроза реализуется, она может взаимодействовать с системой и вызвать нежелательные инциденты, оказывающие неблагоприятное воздействие на систему. В основе угроз может лежать как природный, так и человеческий фактор; они могут реализовываться случайно или преднамеренно. Источники как случайных, так и преднамеренных угроз должны быть идентифицированы, а вероятность их реализации - оценена. Важно не упустить из виду ни одной возможной угрозы, так как в результате возможно нарушение функционирования или появление уязвимостей системы обеспечения безопасности информационных технологий.

Исходные данные для оценки угроз следует получать от владельцев или пользователей активов, служащих отделов кадров, специалистов по разработке оборудования и информационным технологиям, а также лиц, отвечающих за реализацию защитных мер в организации.

После идентификации источника угроз (кто и что является причиной угрозы) и объекта угрозы (какой из элементов системы может подвергнуться воздействию угрозы) необходимо оценить вероятность реализации угрозы.

При этом следует учитывать:

1. частоту появления угрозы (как часто она может возникать согласно статистическим, опытным и другим данным), если имеются соответствующие статистические и другие материалы;
2. мотивацию, возможности и ресурсы, необходимые потенциальному нарушителю и, возможно, имеющиеся в его распоряжении; степень привлекательности и уязвимости активов системы информационных технологий с точки зрения возможного нарушителя и источника умышленной угрозы;
3. географические факторы - такие как наличие поблизости химических или нефтеперерабатывающих предприятий, возможность возникновения экстремальных погодных условий, а также факторов, которые могут вызвать ошибки у персонала, выход из строя оборудования и послужить причиной реализации случайной угрозы.

В зависимости от требуемой точности анализа может возникнуть необходимость разделить активы на отдельные компоненты и рассматривать угрозы относительно этих компонентов.

После завершения оценки угроз составляют перечень идентифицированных угроз, активов или групп активов, подверженных этим угрозам, а также определяют степень вероятности реализации угроз с разбивкой на группы высокой, средней и низкой вероятности.

Оценку угроз осуществляет специалист сторонней организации. Периодичность оценки – один раз в квартал. Оценка осуществляется экспертным методом.

Оценка угроз активам предприятия приведена в таблице 1.4 [5]. При формировании перечня угроз использовался стандарт ГОСТ Р ИСО/МЭК ТО 13335-3-2007.

Таблица 1.4

Оценка угроз активам

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональные данные сотрудников	«1С
1. Угрозы, обусловленные преднамеренными действиями					
Намеренное повреждение					+
Кража	+	+	+	+	+
Несанкционированное использование носителей данных	+	+	+	+	+
Нелегальное проникновение злоумышленников под видом санкционированных пользователей					+
Вредоносное программное обеспечение					
Ошибка операторов					+
2. Угрозы, обусловленные случайными действиями					

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональные данные сотрудников	Акт «1С
Неисправности в системе электроснабжения					
Аппаратные отказы					+
Ошибка обслуживающего персонала					+
Ошибка при обслуживании					+
Программные сбои					+
Ошибка операторов					+
Сбои в функционировании услуг связи					+
3. Угрозы, обусловленные естественными причинами (природные, техногенные ф					
Колебания напряжения					+

Группа уязвимостей Содержание уязвимости	Актив №1: Инструкции по безопасности	Актив №2: Информация о деятельности предприятия	Актив №3: Персональные данные клиентов	Актив №4: Персональные данные сотрудников	Акт «1С
Затопление	+	+	+	+	+

Состав и взаимодействие аппаратных средств, используемых для обработки информационных активов, подлежащих защите:

1. Рабочие станции – 6 единиц;
2. Серверы – 1 единицы.

На рис. 1.1 приведена схема информационной сети предприятия.

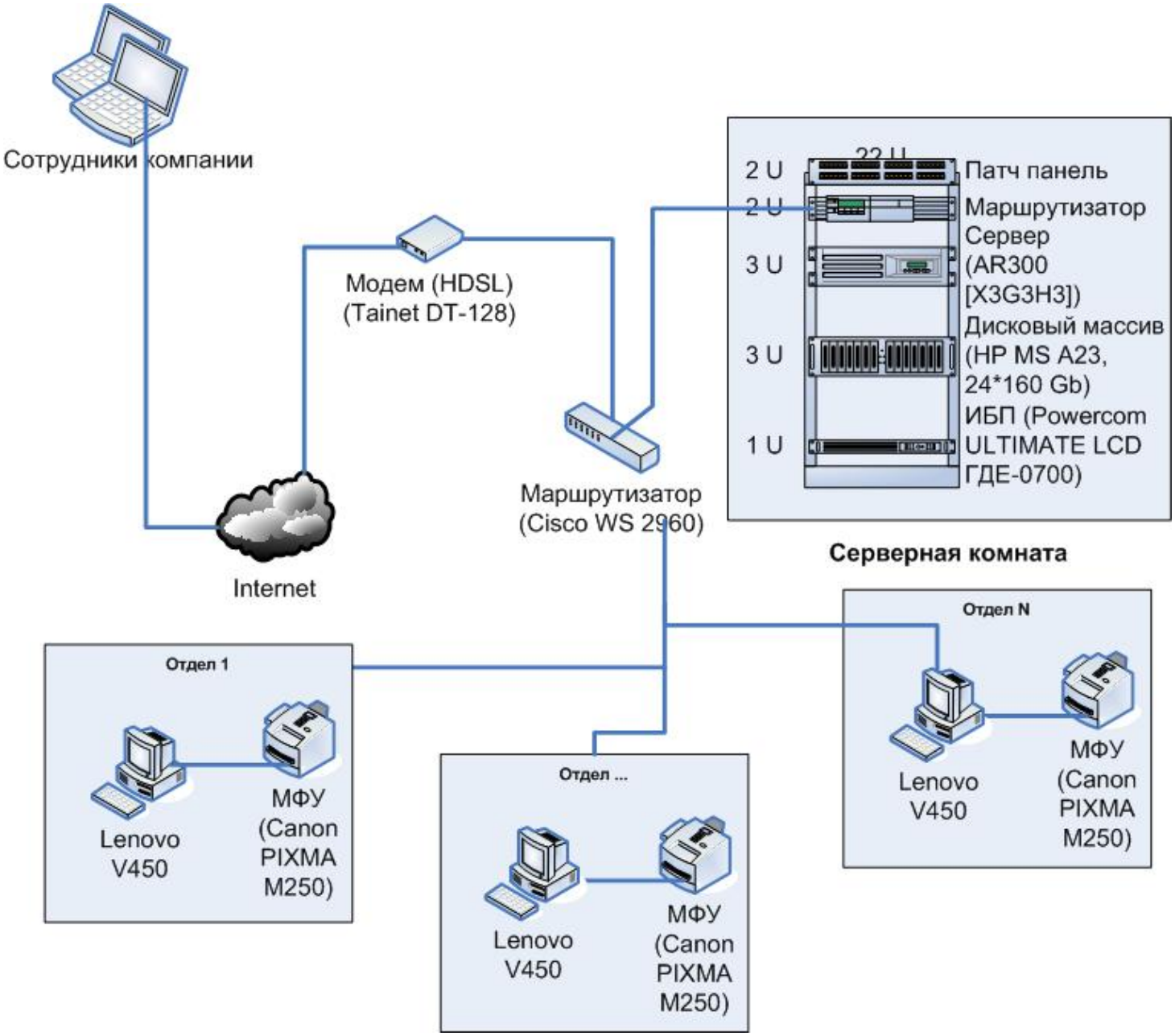


Рис. 1.1 - Схема информационной сети предприятия

Как видно из рисунков рабочие станции объединены в локальную сеть на коммутаторах и имеют выход в интернет через маршрутизатор.

Спецификация оборудования:

Маршрутизатор CISCO WS 2960. Спецификация приведена в таблице 1.5

Таблица 1.5

Спецификация маршрутизатора

Процессор	100-MHz IDT R4700 RISC
Flash-память	От 4 до 32-MB
Оперативная память	От 16 до 128-MB DRAM
Слоты для модулей	4
Консольный и AUX порты (до 115.2 Kbps)	Да
Монтируется на стену или в RACK	Да
Сдвоенные слоты Type II PCMCIA	Да

Рабочие станции Lenovo V450. Спецификация приведена в таблице 1.6.

Таблица 1.6

Спецификация рабочей станции

Процессор	Celeron Processor 450 (2.2 GHz, 512K, 800 MHz)
Оперативная память	1 GB DDR2-800
Жесткий диск	100 GB SATA (7200 rpm)
Видеокарта	256 MB
Сетевая карта	Gigabit Ethernet 10/100/1000Base-TX
Клавиатура	Depo KWD-820 PS/2

Мышь	Depo mouse PS/2 Black
Блок питания	300 Вт

Сервер AR300X3G3H3

- Два четырехядерных процессора Intel® Xeon® 5500 (Nehalem)
- Поддержка технологии Hyper-threading — до 16-ти одновременных вычислительных потоков;
- Технология Turbo boost — повышение частоты процессора при пиковой нагрузке;
- Энергосберегающие режимы — снижение энергопотребления на 50% в «холостом» режиме;
- 32 GB памяти DDR3 1066/1333MHz, интегрированный в процессор контроллер памяти;
- Дисковая подсистема SAS или SATA, до 6-ти жестких дисков с горячей заменой;
- Возможность полного удаленного управления;
- Резервирование по питанию с возможностью горячей замены.

МФУ Canon PIXMA V250. Спецификация приведена в таблице 1.7

Таблица 1.7

Спецификация принтера

Тип принтера	лазерный
Цветность	монохромный
Разрешение	2400x600 dpi
Скорость печати (ч/б)	22 стр./мин.

Время выхода первой страницы	Менее 10 секунд

Процессор

Процессор	181 МГц

Память

Память	32 Мб

Расходные материалы

Формат бумаги	A4
Плотность печатных носителей	60-163 г/м2
Расходные материалы	Картриджи Brother: TN-2135/TN-2175. Фотобарабан DR-2175

Способы подключения и соединения

Интерфейс	USB 2.0 RJ-45 WiFi

Управление бумагой

Емкость подающего лотка	250 л

Размеры и вес

Размеры	368x170x361 мм
Вес	6.8 кг

На рис. 1.2 приведена схема программной архитектуры предприятия.

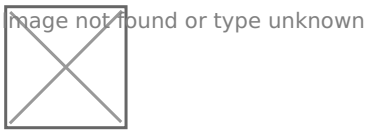


Рис. 1.2 – Схема программной структуры предприятия

Целью оценки рисков является идентификация и оценка рисков, которым подвергаются рассматриваемая система информационных технологий и ее активы с тем, чтобы идентифицировать и выбрать подходящие и обоснованные защитные меры безопасности. Величина риска определяется ценностью подвергающихся риску активов, вероятностью реализации угроз, способных оказать негативное воздействие на деловую активность, возможностью использования уязвимостей идентифицированными угрозами, а также наличием действующих или планируемых защитных мер, использование которых могло бы снизить уровень риска.

Существуют различные способы учета таких факторов (активы, угрозы, уязвимости), например, можно объединить оценки риска, связанные с активами, уязвимостями и угрозами, для того, чтобы получить оценки измерения общего уровня риска. Различные варианты подхода к анализу риска, основанные на использовании оценок, полученных для активов, уязвимостей и угроз.

Вне зависимости от использованного способа оценки измерения риска, результатом оценки, прежде всего, должно стать составление перечня оцененных рисков для каждого возможного случая раскрытия. Составленный перечень оцененных рисков затем используют при идентификации рисков, на которые следует обращать внимание в первую очередь при выборе защитных мер. Метод оценки рисков должен быть повторяемым и прослеживаемым.

Как уже говорилось выше, для ускорения всех или отдельных элементов процесса анализа риска могут использоваться различные автоматизированные программные средства. Если организация решит использовать такие средства, необходимо проследить, чтобы выбранный подход соответствовал принятым в организации стратегии и политике безопасности информационных технологий. Кроме того, следует обратить особое внимание на правильность используемых входных данных, поскольку качество работы программных средств определяется качеством входных данных.

Возможны две методики оценивания рисков. Одна из них направлена на определение наиболее критичных активов в организации с точки зрения рисков ИБ по «штрафным баллам». Другая методика направлена на оценку рисков по степени влияния уязвимостей на бизнес-процессы [7].

В нашем случае целесообразно использование методики направленной на оценку наиболее критичных активов, так как в основе работы предприятия лежит один бизнес-процесс, но в рамках данного бизнес-процесса задействованы активы разных степеней ценности.

Описание проведения процедуры оценки рисков:

1. должностные лица – начальник отдела безопасности, начальники отделов – пользователей активов;
2. способ представления исходной информации – начальникам отделов дается форма с перечнем возможных угроз и уязвимостей, начальники отделов при участии сотрудников отделов заполняют таблицу, оценивая угрозы и уязвимости для своего актива;
3. способ представления результатов оценки рисков – начальник отдела безопасности собирает заполненные формы у начальников отделов и формирует интегральную оценку рисков и ранжирует риски.

Таблица «штрафных баллов» для комбинации ценности активов, уровня угроз и уязвимостей приведена в таблице 1.8

Таблица 1.8

Таблица «штрафных баллов»

	Уровни угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Результаты проведения оценки целесообразно свести в таблицу 1.9, которая должна содержать риски наиболее ценным информационным активам, ранжированные в порядке убывания.

Таблица 1.9

Результаты оценки рисков информационным активам организации

Актив	**Ранг риска**
Инструкции по безопасности	3
Информация о деятельности предприятия	2
Персональные данные клиентов	4
Персональные данные сотрудников	5
Система «1С:Предприятие» (актив программного обеспечения)	4

Сервер БД	1

Результат оценки рисков показал, что наибольшему риску подвержен сервер БД, это связано с тем, что данный актив имеет большее число угроз и уязвимостей, не смотря на то, что данный актив имеет не самый высокий ранг.

Следующим по уровню риска идет информационный актив – информация о деятельности предприятия. Данный актив имеет максимальный ранг.

1.2. Выбор защитных мер информационной безопасности

Для обеспечения информационной безопасности организации выбран следующий перечень организационных мероприятий:

1. Отнесение информации к коммерческой тайне - установление ограничений на распространение информации, требующей защиты;
2. Категорирование помещений производится по степени важности обрабатываемой в них информации;
3. Для каждой информационно-вычислительной системы предприятия, а в отдельных случаях для персональных компьютеров (ПК), определяется категория обрабатываемой в ней информации с учетом «Перечня сведений, составляющих коммерческую тайну компании».
4. Определение факторов риска — возможных ситуаций, возникновение которых может расцениваться как угроза, и способных нанести ущерб материального или нематериального характера;
5. Определения общих правил обработки информации;
6. Определения обязанностей пользователей и персонала систем по защите информации;
7. Разработка плана обеспечения безотказной работы и восстановления сетей и систем организации;
8. Резервное копирование и хранение программ и данных на внешних носителях;
9. Журналирование критичных событий;
10. Резервирование аппаратных ресурсов.

Одним из основных недостатков существующей системы ИБ является отсутствие системы контроля управления доступом и системы видеонаблюдения. К данным системам выдвигается ряд требований [8].

Выбор и установка СКУД для предприятия осуществлялся в соответствии с требованиями ГОСТ Р 51241-98.

В таблице 1.10 представлено сравнение СКУД по функциональным возможностям.

Таблица 1.10

Сравнение СКУД

Характеристики	**Elsys**	**GATE**	**Кронверк**
регистрацию и протоколирование тревожных и текущих событий	5	4	4
приоритетное отображение тревожных событий	5	3	4
управление работой УПУ в точках доступа по командам оператора	5	3	3
задание временных режимов действия идентификаторов в точках доступа «окна времени» и уровней доступа	5	0	3
защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации	3	0	0
автоматический контроль исправности средств, входящих в систему, и линий передачи информации	4	3	4

Характеристики	Elsys	GATE	Кронверк
возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления	4	4	2
установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях	3	3	0
блокировку прохода по точкам доступа командой с пункта управления в случае нападения	4	4	3
возможность подключения дополнительных средств специального контроля, средств досмотра	5	4	4
Интегральная оценка	43	28	27

СКУД Elsys

СКУД Elsys предназначена для автоматического контроля пропускного режима и управления исполнительными устройствами (автоматическими воротами, шлагбаумами, лифтами, турникетами, замками и т.п.) в соответствии с заданными полномочиями и расписаниями.

Автоматизированная СКУД - важнейший инструмент повышения уровня безопасности предприятия и укрепления трудовой дисциплины.

Аппаратной основой системы являются контроллеры Elsys-MB, выпускаемые в различных по характеристикам вариантах исполнения Pro, Pro4, Standard, Light и SM. Наличие этих вариантов, а также модулей расширения памяти различной емкости к ним, позволяет при проектировании оптимизировать технико-экономические характеристики систем различного масштаба.

Контроллеры Elsys-MB объединяются в сеть по двухпроводному интерфейсу RS-485 (до 63 контроллеров в одной линии связи). Линии связи RS-485 подключаются к

серверу оборудования СКУД через преобразователи интерфейсов RS-232/RS-485 или USB/232-485 (до 15 линий на один ПК), либо по компьютерной сети предприятия через коммуникационные сетевые контроллеры (КСК) Elsys-MB-Net (до 256 КСК на один ПК). Кроме того, в системе может быть несколько серверов оборудования, объединенных компьютерной сетью, что обеспечивает практически неограниченные возможности масштабирования системы.

Сочетание ряда технических решений, принятых в системе, придает ей уникальные возможности:

1. высокая производительность и большой объем памяти контроллеров Elsys-MB, обеспечивающие обслуживание большого (до 65 тысяч) числа пользователей и длительную работу (до нескольких суток) в автономном режиме в условиях интенсивного потока событий без потери информации о событиях;
2. высокая отказоустойчивость системы, обусловленная одноуровневой архитектурой;
3. аппаратная реализация функции "глобальный контроль последовательности прохода" (antipassback) в масштабах системы, содержащей до 16128 контроллеров, в том числе и географически распределенной;

Система видеонаблюдения TRASSIR

Система видеонаблюдения TRASSIR представляет собой многофункциональный интегрированный программно-аппаратный комплекс и предназначена для обеспечения непрерывного автоматизированного мониторинга охраняемых объектов с архивацией видео- и аудиоданных.

Оперативность и удобство работы с системой

Интерфейс системы интуитивно понятен и осваивается за несколько минут без подробного изучения инструкции. Установка проста и автоматизирована. Управление просмотром может осуществляться только манипулятором типа мышь или сенсорным экраном. В программе создана эргономичная двухуровневая система настроек, предназначенная для пользователей с разным уровнем подготовки и полномочий. Все настройки системы сгруппированы по уровням сложности. Основной уровень для оператора Предназначен для пользователя ПК, обладающего навыками работы со стандартными приложениями Windows и не имеющего полномочий администрирования системы. Преимуществом этого уровня является мгновенный доступ - для открытия панели настроек этого уровня достаточно щелкнуть правой клавишей мыши по нужному окну видеоканала.

Оператор может регулировать разрешение записи, уровень сжатия, задать скорость ввода, настроить яркость, контрастность и освещенность. Расширенный уровень для администратора и инсталлятора TRASSIR Опытный пользователь, обладающий статусом администратора системы, имеет доступ к системным настройкам и полной информации о работе системы. А инсталлятор, осуществляющий монтаж, настройку и дальнейшее сопровождение продукта, использует этот расширенный уровень как встроенный инструмент диагностики работы системы. Здесь доступны следующие возможности: расширенное управление настройками видеозаписи, мониторинг и диагностика системы в сети, Одновременное управление настройками всех каналов, статистическая сводка о состоянии архивов и емкости хранилищ, отладочный журнал.

Многозадачный режим работы

TRASSIR мультифункциональная система: все операции, включая мониторинг, запись архива, просмотр архива, настройки, доступ по сети, просмотр архива по сети, а также взаимодействие с интегрированными системами безопасности осуществляются параллельно в едином интерфейсе.

Синхронная запись звука

Все модели систем TRASSIR, кроме линейки с программной компрессией, оснащены высококачественной синхронной аудиозаписью по каждому каналу, а некоторые модели семейства IP-видеосерверов TRASSIR Lanser и IP видеокамеры поддерживают дуплексную аудиосвязь.

Удаленная работа по сети

Сетевая архитектура ПО TRASSIR позволяет строить распределенные системы любого масштаба – к одному серверу может подключиться неограниченное количество сетевых клиентов – как по локальной сети, так и по глобальной сети Интернет. Система обеспечивает не только просмотр текущих событий, но и полноценный доступ к архивам, отвечающий требованиям безопасности данных. В системе реализовано удаленное администрирование и управление поворотными камерами. Программа «Клиент», обеспечивающая доступ к видеосерверу с удаленного рабочего места, распространяется бесплатно и предусматривает неограниченное количество сетевых клиентов.

Детектирование движения

В арсенале пользователя системы целый набор детекторов движения и фильтров. В TRASSIR предусмотрены два детектора: базовый Generic Detector и специальный детектор объектного трассирования SIMT (Simple Intelligent Motion Trassir). Возможности Generic Detector: детектирование медленного и быстрого движения, выставление произвольных зон детектирования, детектирование лиц, детектирование расфокусировки, детектирование сдвига, ослепления видеокамеры, закрытия её рукой. Все эти функции создают события в журналах TRASSIR, тревожные сообщения оператору и по ним в дальнейшем можно осуществлять поиск Детектирование лиц, другие специальные детекторы. TRASSIR предлагает бесплатно уникальный функционал – детектор лиц в поле зрения камеры, а так же специализированные детекторы смещения, засветки и закрытия (саботажа) видеокамеры. Возможности детектора объектного трассирования SIMT: показывает отличные результаты в при уличном применении и в сложных погодных условиях, эффективно фильтрует случайные шумы, селектирует объекты по размерам, направлению, скорости движения, обеспечивает детектирование только объектов с заданными параметрами и аналитическое предсказание дальнейшей траектории движения объекта с помощью вектора скорости, применяется в автоматическом режиме работы функции ActiveDome+.

Также предусмотрены дополнительный детектор медленного движения и детектор оставленных предметов.

Запись по расписанию

Командная структура записи по расписанию позволяет задать интервалы записи в произвольном порядке и с дополнительными параметрами. Расписание устанавливается на календарную неделю и будет циклично повторяться каждую неделю.

Многоуровневый доступ

В программном обеспечении TRASSIR реализована многоуровневая система распределения прав доступа – возможность создания пользователей с различными правами доступа (например, только просмотр текущих событий, просмотр + просмотр архива, возможность менять настройки системы и т.д.) Эта функция позволяет предотвратить несанкционированный доступ к системе.

Журнал событий

Журнал событий предоставляет операторам и администраторам возможности по просмотру и поиску системных тревожных и информационных уведомлений. Все события сохраняются в БД TRASSIR для дальнейшего их поиска и анализа, пользователи журнала могут сохранять собственные фильтры как для online режима, так и для поиска в БД. С помощью гибкой системы фильтров каждый оператор журнала TRASSIR сможет найти важную для себя информацию согласно собственным критериям.

Архивирование видеоданных

Запись видеоданных на внутренние дисковые накопители производится по циклическому принципу, когда текущие данные заменяют самые старые. Используется прогрессивная технология "MultiStor": при наличии нескольких накопителей запись с каждой камеры ведется одновременно на все, повышая надежность и снижая нагрузку на каждый накопитель в отдельности. За счет этого в случае выхода из строя одного из накопителей, информация на других сохраняется. В настройках записи в архив можно указывать объем оставляемого места на диске, какой объем информации удалять за один раз, какой объем места может занимать архив, а также предусмотрена система диагностики и статистики свободного места на каждом из накопителей. Каждый пользователь сможет оценить мгновенный доступ к архиву. Фрагменты из архива можно просматривать в любом порядке, прокручивать вперед и назад, увеличивать и уменьшать скорость просмотра, просматривать покадрово, создавать снимки в форматах *.BMP или *.JPG. Осуществляется запись по расписанию и по детекции, предусмотрена предзапись и дозапись. TRASSIR поддерживает неограниченное количество жестких дисков для записи. Системой поддерживается горячее отключение и подключение цифровых носителей, в том числе и такие популярные и недорогие как CD, USB-накопители и Fire Wire. Можно копировать отдельные кадры или целые фрагменты видеозаписей. Просмотр архивов без TRASSIR. Во-первых, в комплекте с системой бесплатно поставляется внешний плеер архива (несколько вариантов для разных систем). Во-вторых, вы можете установить специальный кодек для основного формата системы – H.264 и проигрывать видео со звуком в Windows Media Player. И, в-третьих, с помощью бесплатной утилиты, сконвертировать H.264 файлы системы в .avi или .wmv формат, читаемый на любом компьютере как с помощью Windows Media Player, так и другими средствами просмотра. Встроенные в систему и поставляемые в комплекте внешние плееры, позволяют вырезать нужные части из видеофрагментов, делать скриншоты и проверять сохранность H.264 видео (для защиты от редактирования – проверка на watermark).

Редактор шаблонов

Расположение видеоканалов на основном мониторе можно создавать произвольно, используя редактор шаблонов. Вы можете создать неограниченное количество шаблонов – различных комбинаций как локальных так и сетевых каналов, ip-видео каналов и планов помещений. Каждому отдельному окну можно самостоятельно задать свою камеру путем её перетаскивания в форму окна (drag&) при редактировании. На дополнительных мониторах можно комбинировать любые IP системы, программные системы и планы. На MDI мониторах – только H.264 видео (1 канал на монитор) или до 16 каналов предпросмотра несжатого видео с аппаратных плат.

Правила

В системе TRASSIR предусмотрена возможность задания реакции на определенные события. Благодаря этой возможности, пользователь может установить на любое событие индивидуальную реакцию или несколько типов реакции: включение/выключение записи, изменение скорости записи, звуковые сигналы, отправка СМС, наведение поворотных видеокамер на объект и т.д. Поддерживаются каскадные правила – множественные реакции с заданной задержкой на одно событие. Возможность подключения тревожных входов и выходов Используя в качестве аппаратной платформы IP-видеосерверы Lanser4M/4HDD/1Real, IP-камеры, можно с минимальными затратами дополнить имеющуюся систему видеонаблюдения охранно-пожарной подсистемой путем подключения датчиков к тревожным входам и выходам. При больших системах становится рентабельным использование интегрированных систем типа Болид в качестве тревожных входов и выходов. Informer – сервис оповещения о тревожных событиях. В программе предусмотрено несколько каналов оповещения: индивидуальные звуковые сигналы для каждого типа событий, отправка писем по электронной почте, отсылка SMS на мобильный телефон. Пользовательский интерфейс функции максимально прост для понимания, не требуется настройка внешних почтовых программ. Информер так же отвечает за проигрывание звуковых сообщений, которые можно задавать индивидуально для любого события. Управление телеметрией (PTZ) TRASSIR поддерживает управление любыми моделями поворотных камер, которые поддерживают наиболее распространенные протоколы Pelco-P или Pelco-D, а так же видеокамерами таких производителей как Lilin, Samsung, Pelco, CNB и Hitron, Infinity и Tedd. Если модели камер других производителей поддерживают любые из выше перечисленных протоколов, ими также можно управлять. Для удобства пользователей предусмотрено управление с

помощью цифровой панели компьютерной клавиатуры.

Кроме этого, TRASSIR обладает уникальной патентованной системой управления скоростными поворотными камерами – ActiveDome.

Регулирование качества архивного видео - степени компрессии видеоинформации

Возможность задания оптимального соотношения объема и качества видеозаписи и занимаемого объема, выбирая степень компрессии из десятков вариантов, делая это двумя способами – простым (выбирая по принципу лучше-хуже) или настраивая максимально подробно в системном меню (для системных администраторов системы).

Поддержка многомониторного режима работы

Базовая бесплатная поддержка до 8 VGA мониторов, опциональная поддержка до 32 аналоговых CCTV мониторов (требуется приобрести платы MDI). Подробнее СПЕЦИАЛЬНЫЕ ВОЗМОЖНОСТИ Функция интерактивного управления поворотными видеокамерами Active Dome позволяет оператору одним кликом мыши увеличить нужный объект в 15-20 раз, не прерывая общего наблюдения.

ГЛАВА 2. АНАЛИЗ ПРАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Комплекс проектируемых программно-аппаратных средств

Аппаратно-программные средства защиты информации предоставляются устройствами, встраиваемыми непосредственно в аппаратуру АИС, или устройствами, сопряженными с аппаратурой АИС по стандартному интерфейсу и предназначенными для реализации конкретных функций защиты. Они реализуют логическую оболочку АИС, ориентированную на обеспечение безопасности [8].

Программно-технические методы и средства обеспечения информационной безопасности:

1. Системы разграничения доступа – для физического разграничения доступа в помещениях предприятия будет использован СКУД «Elsys», для программного разграничения доступа в информационной системе предприятия будет использовано программное средство Microsoft Active Directory;
2. Система контроля за действиями посетителей и сотрудников - система видеонаблюдения TRASSIR;
3. Средства восстановления работоспособности АС – для восстановления работоспособности операционной системы на рабочих станциях и серверах будет использовано программное средство Microsoft Data Protection Management License – средство для резервного копирования и архивации для файловых серверов, представляет собой серверное приложение, предназначенное для оптимизации резервного копирования данных и их восстановления с использованием жестких дисков;
4. Средство антивирусной защиты – для защиты корпоративной сети от вирусов будет использован пакет Kaspersky IS 8.0.
5. Генератор шума ГШ-2500 – средство для защиты от прослушивания.
6. «Сонаты - Р2» - система защиты объектов информатизации от утечки по техническим каналам.
7. Средства мониторинга – для мониторинга работы системы будет использовано программное средство Microsoft Operations Manager 2007.

СКУД «Elsys» и система видеонаблюдения «TRASSIR» устанавливается поставщиком данной системы. Компания-поставщик проводит обучающие семинары с сотрудниками службы безопасности организации, осуществляет сервисное обслуживание.

Настройку программных средств осуществляет официальный поставщик ПО компании Microsoft. Все штатные средства ОС Windows также устанавливают сотрудники компании-поставщика.

Генератор шума ГШ-2500 устанавливается в зале совещаний и включается при проведении конфиденциальных переговоров.

Сонаты - Р2 устанавливается в помещениях предприятия.

Сотрудники отдела безопасности и информационно-технического отдела проходят специальное обучение использования данных программных средств и в дальнейшем работают с ними самостоятельно.

За исправное состояние программных средств несет ответственность дежурный системный администратор.

За исправность технических средств охраны несет ответственность сотрудник отдела безопасности – дежурный начальник смены.

2.2 Выбор и обоснование методики расчёта экономической эффективности

Исходной посылкой при экономической эффективности является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой - обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и потерь от ее нарушения.

Очевидно, что оптимальным решением было бы выделение на защиту информации средств, минимизирующих общую стоимость работ по защите информации.

Также очевидно, что экономическая эффективность мероприятий по защите информации может быть определена, через объем предотвращенного ущерба или величину снижения риска для информационных активов организации.

Для определения экономического эффекта от внедрения системы ИБ на предприятии воспользуемся первым вариантом (через объем предотвращенного ущерба), так как известны ожидаемые потери при нарушении защищенности информации и зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

Для определения уровня затрат Ri нам известен: перечень угроз информации, потенциальную опасность для информации для каждой из угроз, размеры затрат, необходимых для нейтрализации каждой из угроз.

Для определения уровня затрат возможно использование эмпирической зависимости ожидаемых потерь (рисков) от i-й угрозы информации, формула

$$R_i = 10^{(Si + Vi - 4)} \quad (3.1)$$

где

S_i – коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;

Vi – коэффициент, характеризующий значение возможного ущерба при ее возникновении.

Значения коэффициентов S_i и V_i, приведенные в таблице 2.1 и 2.2.

Таблица 2.1

Значения коэффициентов ***S_i***

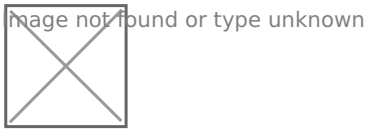
Ожидаемая (возможная) частота появления угрозы	**Предполагаемое значение *S_i***
Почти никогда	0
1 раз в 1 000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 2.2

Значения коэффициентов ***Vi***

Значение возможного ущерба при проявлении угрозы, руб.	**Предполагаемое значение *Vi***
30	0
300	1
3 000	2
30 000	3
300 000	4
3 000 000	5
30 000 000	6
300 000 000	7

Суммарная стоимость потерь определяется формулой 2.2



R=

где

N – количество угроз информационным активам,

R_i – стоимость потерь от реализации угрозы к активу.

Результаты расчетов для активов предприятия представлены в таблице 2.3.

Таблица 2.3

Величины потерь (рисков) для критичных информационных ресурсов

до внедрения/модернизации системы защиты информации

Актив	**Угроза**	**Величина потерь (тыс.руб.)**
Инструкции по безопасности	Намеренное повреждение	900
	Кража	1400
Информация о деятельности предприятия	Кража	2400
	Несанкционированное использование носителей данных	700
	Нелегальное проникновение злоумышленников под видом санкционированных пользователей	800
	Ошибка операторов	60
Персональные данные клиентов	Кража	150
Персональные данные сотрудников	Кража	90

Актив	Угроза	Величина потерь (тыс.руб.)
Сервер БД	Намеренное повреждение	60
	Вредоносное программное обеспечение	30
	Неисправности в системе электроснабжения	10
	Аппаратные отказы	10
	Ошибка обслуживающего персонала	5
	Ошибка при обслуживании	5
	Программные сбои	5
	Ошибка операторов	5
	Сбои в функционировании услуг связи	5
	Колебания напряжения	2
	Затопление	60
Система «1С: Предприятие»	Намеренное повреждение	10
	Кража	10

Актив	Угроза	Величина потерь (тыс.руб.)
Вредоносное программное обеспечение	10	
Ошибка операторов	6	
Ошибка обслуживающего персонала	6	
Ошибка при обслуживании	6	
Программные сбои	6	
Сбои в функционировании услуг связи	6	
Суммарная величина потерь		6757

2.3 Расчёт показателей экономической эффективности проекта

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы.

Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатации и других расходов.

Наиболее общей формой представления ресурса является денежная мера.

Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер.

Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники.

Постоянный ресурс — на заработную плату сотрудникам службы безопасности и поддержание определенного уровня безопасности, прежде всего, путем эксплуатации технических средств и контроля эффективности защиты.

Для определения экономической эффективности системы защиты информации предприятия необходимы следующие данные:

- расходы (выделенные ресурсы) на создание/модернизацию данной системы и поддержание её в работоспособном состоянии;
- величины потерь (рисков), обусловленных угрозами информационным активам после внедрения/модернизации системы защиты информации.

Содержание и объеме разового ресурса, выделяемого на защиту информации, приведен в таблице 2.4.

Таблица 2.4

Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия			
№ п\п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб.)**	**Трудоемкость операции (чел.час)**	**Стоимость, всего (руб.)**

1	Установка СКУД «Elsys»	150	100	15000
2	Проведение обучающих занятий с сотрудниками предприятия	200	40	8000
3	Установка системы видеонаблюдения «TRASSIR»	200	80	16000
4	Проведение обучающих занятий с сотрудниками предприятия	200	20	4000
5	Установка Сонаты - Р2	200	5	1000
6	Установка генератора шума ГШ 2500	200	5	1000
7	Настройка Microsoft Data Protection Management License	200	8	1600
8	Настройка Microsoft Operations Manager 2007	200	8	1600
9	Установка и настройка Kaspersky IS 8.0	200	8	1600
Стоимость проведения организационных мероприятий, всего				91800

Перечень затрат на ПиАСИБ приведен в таблице 2.5.

Таблица 2.5

Перечень затрат на ПиАСИБ

№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
СКУД «Elsys»				
1	Усиленный электромоторный системный турникет	60000	2	120150
2	Программный модуль «Барьер»	40000	1	40000
3	Универсальный контроллер - интерфейсный модуль	8000	1	8000
4	Считыватель бесконтактных карт доступа	2200	30	66000
5	Генератора шума ГШ 2500	15000	1	15000
6	Соната – Р2	15000	2	30000
Стоимость проведения мероприятий инженерно-технической защиты				279000

Объем разового ресурса, выделяемого на защиту информации	370800

Объеме постоянного ресурса, выделяемого на защиту информации, приведен в таблице 2.5.

Таблица 2.5

Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия

№ п\п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб.)**	**Трудоемкость операции (чел.час)**	**Стоимость, всего (руб.)**
1	Дежурство по ТСО	100	720	72015
2	Дежурство администратора сети	200	270	54000
3	Аудит работы ИС	200	30	6000
4	Выполнение плановых мероприятий по ИБ	200	10	2015
5	Выполнение плановых мероприятий по ТСО	200	15	3000

Стоимость проведения организационных мероприятий, всего	137000

Мероприятия инженерно-технической защиты

№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (руб)	Кол-во (ед.измерения)	Стоимость, всего (руб.)
1	Запасные считыватели бесконтактных карт доступа	2200	5	11000
2	Резервные рабочие станции	20150	10	201500
3	Резервные сервера	60000	1	60000
4	Резервные датчики пожарной сигнализации	300	20	6000
5	Резервные датчики охранной сигнализации	200	20	4000
6	Резервные носители информации	3000	4	12015
7	Резервные БСК	300	30	9000
Стоимость проведения мероприятий инженерно-технической защиты				302015

Объем постоянного ресурса, выделяемого на защиту информации	439000

Суммарный объем выделенного ресурса составил: 370800+439000= 809800 рублей (данные взяты из таблиц 2.4 и 2.5 – суммарный размер разового и постоянного ресурсов).

Рассчитанная величина ущерба составила: 6757000 рублей (данная величина взята из таблицы 2.3).

Тем не менее, часть угроз является маловероятными и ими можно пренебречь, таковыми, например, являются стихийные бедствия (потопы, ураганы).

Величина потерь для активов предприятия после внедрения системы ИБ приведена в таблице.

Таблица 2.6

Величины потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации системы защиты информации

Актив	**Угроза**	**Величина потерь (тыс.руб.)**
Инструкции по безопасности	Намеренное повреждение	400
	Кража	20
Информация о сделках	Кража	80
	Несанкционированное использование носителей данных	70

Актив	Угроза	Величина потерь (тыс.руб.)
Нелегальное проникновение злоумышленников под видом санкционированных пользователей	80	
Ошибка операторов	60	
Персональные данные клиентов	Кража	50
Персональные данные сотрудников	Кража	60
Сервер БД	Намеренное повреждение	50
	Вредоносное программное обеспечение	20
	Неисправности в системе электроснабжения	10
	Аппаратные отказы	10
	Ошибка обслуживающего персонала	5
	Ошибка при обслуживании	5

Актив	Угроза	Величина потерь (тыс.руб.)
Программные сбои	5	
Ошибка операторов	5	
Сбои в функционировании услуг связи	5	
Колебания напряжения	2	
Затопление	60	
Система «1С: Предприятие»	Намеренное повреждение	5
	Кража	5
	Вредоносное программное обеспечение	5
	Ошибка операторов	4
	Ошибка обслуживающего персонала	4
	Ошибка при обслуживании	4
	Программные сбои	4

Актив	Угроза	Величина потерь (тыс.руб.)
Сбои в функционировании услуг связи	4	
Суммарная величина потерь		1032

Динамику величин потерь за 2 года с использование СЗИ и без использования СЗИ приведена в таблице 2.7 (данные за первый год взяты из таблиц 2.3 и 2.6).

Таблица 2.7

Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До внедрения СЗИ	1689250	3378500	5067750	6757000	8446250	10135500	11824750	13514000
После внедрения СЗИ	258000	516000	774000	1032015	1290000	1548000	1806000	2064000
Снижение потерь	1431250	2862500	4293750	5725000	7156250	8587500	10018750	11450000

Таким образом, период окупаемости, рассчитываемый по формуле

$$\mathbf{T_{ок} = R_{\Sigma} / (R_{ср} - R_{прогн}) \ (2.3)}$$

где

$\mathbf{R_{\Sigma}}$ - суммарный объем выделенного ресурса;

$R_{ср}$ **–** средняя суммарная стоимость потерь за 2 года (среднее арифметическое 1 строки таблицы 3.7);

$R_{прогн}$ - суммарная стоимость потерь (данная величина взята из таблицы 3.3)

Составляет Ток = 764800 / (7601625 - 6757000) = 684000 / 844625= 0,81 года

ЗАКЛЮЧЕНИЕ

Целью данной работы является обеспечение нормального функционирования предприятия путем разработки политики безопасности и расчета стоимости рисков.

В ходе достижения поставленной цели были выполнение следующие задачи:

1. Проведен анализ предметной области;
2. Проведен анализ активов организации и отранжировать их;
3. Проведен анализ угроз и уязвимостей для каждого актива;
4. Проведен анализ программно-технической архитектуры организации;
5. Проведен анализ существующих технических средств охраны;
6. Разработан перечень решений по правовому, инженерному и организационному обеспечению ИБ;
7. Проведено экономическое обоснование проекта ИБ.

На первом этапе проводился анализ информации, циркулирующей в организации, системы безопасности организации, а также анализ угроз и уязвимостей информации.

Все активы предприятия отранжированы по ценности, определены угрозы и уязвимости для каждого актива.

Описана программная и техническая архитектура организации, описаны существующие технические средства охраны (пожарная и охранная сигнализация).

Далее даны решения по инженерному и организационному обеспечению системы ИБ.

Во второй главе дан анализ правовых основ обеспечения информационной безопасности в организации, описана структура программно-аппаратного комплекса системы ИБ.

В третьей, было приведено технико-экономическое обоснование внедряемой системы защиты и рассчитаны сроки ее окупаемости.

СПИСОК ЛИТЕРАТУРЫ

1. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/Под ред. Акад. РАН Б.Н. Топорникова. - СПб.: Издательство «Юридический центр Пресс», 2016.
2. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: 2015.
3. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: Учебное пособие для ВУЗов. – М.: Радио и связь, 2015. – 192с.
4. Диева С.А., Шаеаева А.О. Организация и современные методы защиты информации. — М: Концерн «Банковский Деловой Центр», 2014.
5. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368с.
6. Козлачков П.С., Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2014.- 736 с.
7. Леваков Г.Н., Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2014.- 256 с.
8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных.— М., 2013. Ч. 1,2.
9. Горбатов В.С, Кондратьева Т. А. Информационная безопасность. Основы правовой защиты. — М., 2013.
10. Соколов Д.Н., Степанюк А. Д., Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2015.- 456 с.
11. Сыч О.С., Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2016.- 736 с.
12. Закон Российской Федерации «О государственной тайне» от 21.07.93 №5485-1.
13. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2016г. № 149-ФЗ;
14. Закон Российской Федерации «О персональных данных» от 27.07.2016г. № 152-ФЗ.

15. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2015 г. № Пр.-1895.
16. Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2015 г. №24.
17. Указ Президента Российской Федерации от 06.03.97 г. № 188 «Перечень сведений конфиденциального характера».
18. Указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.95 №1203.
19. «Положение о сертификации средств защиты информации». Утверждено постановлением Правительства Российской Федерации от 26.06.95 №608.
20. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».
21. ГОСТ 29339-92 «Информационная технология. Защита информации от утечки за счет ПЭМИН при её обработке средствами вычислительной техники. Общие технические требования».
22. ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний».
23. ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения».
24. ГОСТ Р 51583-2015 «Порядок создания автоматизированных систем в защищенном исполнении».
25. ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».