МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

АЗЕРБАЙДЖАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

«ЦЕНТР МАГИСТРАТУРЫ»

На правах рукописи

Ганизаде Ниджат Рамиз оглы

МАГИСТРСКАЯ ДИССЕРТАЦИЯ

На тему: «Проблемы обеспечения безопасности современного бизнеса»

Шифр и название направления: **060409 «Организация и управление бизнесом»**

Специализация: **«Бизнес администрирование»**

Научный руководитель:

к.э.н. доц. **Самедова Э.Р.**

Руководитель магистрской

программы к.э.н. доц. **Аббасова Р.А.**

Зав.кафедрой:

К.э.н. доцент **Алиев М.А.**

Баку 2014

Введение

Актуальность темы. На современном этапе развития экономики в Азербайджанской Республике неотъемлемым атрибутом эффективного осуществления бизнес деятельности выступает обеспечение безопасности бизнеса. Сущность деятельности по обеспечению безопасности бизнеса сводится к своевременному выявлению и нейтрализации угроз экономическому благополучию фирмы, что способствует достижению устойчивого и максимально эффективного функционирования фирмы в настоящее время и высокого потенциала развития бизнеса в будущем.

Обеспечение безопасности бизнеса не может быть одноразовым актом, это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких и слабых мест и потенциально возможных угроз бизнесу. Безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла предпринимательской деятельности. Все это, безусловно, актуализирует проблемы обеспечения безопасности бизнеса в современных условиях

Цель исследования – на основании анализа методов организации безопасности бизнеса разработать научно обоснованные рекомендации по дальнейшему разрешению проблем обеспечения безопасности современного бизнеса.

Задачи исследования. Для достижения поставленной цели требуется решить следующие задачи:

- определить сущность угроз безопасности бизнес деятельности в современных условиях;

- рассмотреть безопасность бизнеса как целостную систему

- изучить зарубежные модели обеспечения безопасности бизнеса

- описать методологические подходы к организации безопасности банка

- пранализировать проблемы обеспечения безопасности бизнеса на примере банка

- проанализировать информационную составляющею организации безопасности бизнес деятельности

- разработать рекомендации по совершенствование механизмов обеспечения безопасности современного бизнеса

Предметом исследования являются механизмы обеспечения безопасности современной бизнес деятельности.

А **объектом исследования** является кредитно-финансовая организация «**ОАО Банк ВТБ (Азербайджан)»**.

Методология исследования базируется на эмпирических обобщениях, методах системного анализа, на изучении литературы зарубежных экономистов.

Научная новизна исследования состоит в том, что:

1. раскрыты объективные цели системы безопасности бизнес структуры и ее основные элементы;
2. проанализированы зарубежные модели обеспечения безопасности бизнеса;

3. определено, что основополагающими целями системы безопасности бизнес единицы являются прогнозирование угроз, формирование системы мер по их предупреждению и ослаблению.
4. разработана система противодействия мошенничеству в банке.

Практическая значимость диссертационной работы заключается в том, что содержащиеся в нем методологические положения и рекомендации по обеспечению безопасности бизнес структур создают предпосылки для совершенствования системы противодействия угрозам имущественной безопасности организации со стороны собственного персонала, обучения сотрудников работе с конфиденциальной информацией, эффективной мотивация сотрудников, минимизации утечек информации при увольнении сотрудника и внедрении комплексной системы защиты информации.

Результаты работы первоначально получили отражение в выполненных рефератах.

Апробация работы. Основные моменты, отмеченные в диссертации, докладывались на семинарских занятиях.

Объем и структура исследования. Диссертация состоит из введения, трех глав, содержащих 9 параграфов, заключения, списка использованной литературы. Объем работы 92 страницы, включающий - 4 рисунка и 5 таблиц.

ГЛАВА I. Теоретико-методологические основы обеспечения безопасности бизнеса

1.1. Угрозы безопасности современного бизнеса

Поисковая система Google на запрос «безопасность это…» выдает более 1 млн. ссылок [35]. Наиболее универсальным определением, по нашему мнению, является следующее: безопасность — это такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению или невозможности ее функционирования и развития.

Под безопасностью бизнеса понимается состояние защищенности жизненно важных интересов бизнеса от внутренних и внешних угроз.

К жизненно важным интересам отнесена совокупность потребностей, удовлетворение которых обеспечивает устойчивое достижение целей организации, где:

Потребность - нужда, принявшая свои специфические формы под действием культурных, социальных, политических и других факторов.

Нужда - острая нехватка чего-либо.

Организация - два или более человека объединенные одной целью.

Формулировка «цель бизнеса» требует отдельного пояснения.

Сформировалось два подхода к определению того, что же является основной целью бизнеса:

Американский подход - главная цель - максимизация прибыли на долгосрочной основе. Японский подход - главная цель – максимизация качества продукции и получение максимума прибыли на этой основе.

Все определения понятия «безопасность», которые даются в различных литературных источниках в прямом или косвенном виде включают следующие основные положения:

• наличие угроз, подразделяющихся в свою очередь на внешние угрозы и внутренние;

• наличие жизненно важных интересов объектов защиты;

• баланс интересов между ними.

Первичным в предложенных определениях является именно наличие угроз. Вторичный аспект — наличие жизненно важных интересов, т. е. тех интересов, реализация которых определяет само существование объектов защиты и без которых объекты перестают существовать как единое целое. Например, для государства — это суверенитет и целостность границ, экономический рост; для предприятия — эффективная текущая деятельность и устойчивые тенденции развития. Что касается баланса интересов, то это категория хотя и подчиненная, но также крайне важная, так как без соблюдения такого баланса возникает угроза появления интересов одного из объектов защиты в ущерб другим.

Угрозы объектам безопасности, исходящие от внутренних и внешних источников опасности, определяют содержание деятельности по обеспечению внутренней и внешней безопасности. Если учитывать, что внешние и внутренние угрозы различаются как реальные и потенциальные, то деятельность по обеспечению безопасности будет сводиться к прогнозированию угроз, определению и реализации наиболее эффективных мер по их локализации. Отсюда следует, что основой организации, планирования и реализации мер обеспечения безопасности в различных сферах являются анализ и оценка характера реальных и потенциальных внутренних и внешних угроз, кризисных ситуаций, а также прочих

неблагоприятных факторов, препятствующих достижению поставленных целей и представляющих опасность для жизненно важных интересов.

На уровне промышленного предприятия в значительной степени проявляется зависимость от субъективных факторов, так как концепцию достаточности безопасности конкретного предприятия определяет его руководство исходя из своего представления о проблеме безопасности, наличия необходимых для ее обеспечения ресурсов, стратегических целей деятельности.

Очевидно, что, обосновывая затраты на обеспечение экономической безопасности, необходимо учитывать все три составляющие, отмеченные как общие в большинстве определений, а также недетерминированный характер угроз. Система реальных и потенциальных угроз экономической безопасности не статична. Угрозы могут появляться и исчезать, нарастать и уменьшаться. К тому же субъекты отношений безопасности (человек, общество, предприятие, регион, государство) — сложные многоцелевые системы, определить потребность в безопасности которых весьма затруднительно.

Угрозу безопасности бизнеса можно трактовать как любой конфликт целей функционирования и развития бизнеса с внешней или внутренней средой, а если цели совпадают — как несовпадение путей их достижения. Иными словами, угроза безопасности бизнеса — совокупность условий и факторов, создающих опасность его жизненно важным интересам (производственным мощностям, технологии, менеджменту, работникам и т.д.).

Предложенные определения позволяют рассматривать систему обеспечения безопасности бизнеса как комплекс эффективных мер (управленческих решений) по локализации реальных и потенциальных внутренних и внешних угроз. Этот комплекс мер должен быть обоснован

оценкой характера этих угроз, анализом кризисных ситуаций, прочих неблагоприятных факторов, препятствующих достижению целей предприятия и представляющих опасность для его жизненно важных интересов.

Баланс жизненно важных интересов предприятия должен подразумевать соответствие располагаемого ресурсно-производственного потенциала (производственной мощности, активов, доли рынка, наличия стратегических зон хозяйствования, вида кривой жизненного цикла) формулируемым стратегическим целям его развития. Еще может оказаться, что необходимость обеспечения безопасности объекта возникает в результате появления такой функции его деятельности, которая ранее не предусматривалась (например, производство нового вида продукции или оказание нового вида услуг). И тогда также можно говорить об определенной модели эффективного функционирования и развития.

В систематизации угроз мы будем использовать следующие признаки, встречающиеся в наиболее известных классификациях: виды угроз, их объекты — направления, субъекты — источники, методы и средства защиты от них.

По видам угрозы чаще всего подразделяют на два основных класса:

1)естественные (объективные);

2)искусственные (субъективные).

Естественные угрозы вызываются стихийными природными явлениями (землетрясениями, наводнениями, ураганами).

Искусственные угрозы вызваны деятельностью человека. Они могут иметь непреднамеренный или, наоборот, преднамеренный характер.

Непреднамеренные (непредумышленные) угрозы вызываются ошибками, например, в проектировании производственных систем или в их

эксплуатации. Субъектов таких угроз принято называть нарушителями. На промышленных предприятиях недостаточная квалификация или нарушение ими должностных инструкций могут вызвать такие проявления непреднамеренных угроз:

- травмы и гибель людей;
- повреждение оборудования, линий связи, каналов жизнеобеспечения;
- нерациональное изменение технологий;
- нерегламентированное использование технических средств, документов, компьютерных программ;
- разглашение конфиденциальной информации;
- некомпетентное использование, некорректную настройку или неправомерное отключение персоналом средств защиты службы безопасности.

Субъектов преднамеренных (умышленных) угроз называют злоумышленниками. Угрозы вызываются их корыстными устремлениями (терроризмом, забастовками, хищениями, кражами) и могут привести к травмам и гибели людей. К проявлениям умышленных угроз также относят:

- физическое разрушение объекта или отдельных его элементов в результате терроризма, хулиганства, вандализма; отключение или вывод из строя систем жизнеобеспечения объекта вследствие тех же причин;
- действия по дезорганизации функционирования объекта (забастовки, саботаж, постановка помех);
- хищение материальных ценностей;
- съем информации путем контроля каналов связи, негласной установки специальных технических средств, анализа и контроля побочных излучений, негласных видео- и фотосъемок;
- хищение документов, магнитных носителей и бумажных отходов (распечаток, копировальной бумаги).

Перечисленные угрозы по отношению к защищаемому объекту также могут быть внешними и внутренними. Например, выброс радиоактивных веществ даже далеко за территорией охраняемого объекта может, тем не менее, нанести ему ущерб. В случаях, когда источник внешней угрозы установить затруднительно, ее относят к стихийным бедствиям.

Можно предложить общую классификацию видов и субъектов умышленных угроз (табл.1.1.).

Учитывая, что сами угрозы не являются равнозначными по последствиям проявлений, т. е. их значимость определяется возможными последствиями, целесообразна классификация их по степени важности.

Таблица 1.1.

Классификация угроз по видам и субъектам

Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				внутр	вне
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудования и техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

В классификации угроз по объектам особое значение имеют информационные угрозы. Здесь может быть использована классификация умышленных информационных угроз, отвечающая требованиям безопасности автоматизированных систем обработки информации и приведенная в таблице 1.2.

Таблица 1.2.

Классификация информационных угроз

Принцип классификации	Виды вероятных угроз
По цели воздействия на АСОИ	• нарушение конфиденциальности информации • нарушение целостности информации • нарушение (частичное или полное) работоспособности АСОИ
По принципу воздействия	• с использованием доступа субъекта системы к объекту угрозы
По характеру воздействия на АСОИ	• активное воздействие • пассивное воздействие (бездействие)
По причине появления используемой ошибки защиты	• неадекватность политики безопасности реалиям АСОИ • ошибки административного управления • ошибки в алгоритмах и программах
По способу воздействия на объект угрозы (при активном воздействии)	• непосредственное воздействие на объект угрозы • воздействие на систему разрешений • опосредованное воздействие (через других пользователей) • «маскарад» (присвоение прав другого пользователя)
По способу воздействия на АСОИ	• в интерактивном режиме • в пакетном режиме
По объекту угрозы	• АСОИ в целом • объекты АСОИ • субъекты АСОИ
По используемым средствам реализации	• вирусы • программные ловушки
По состоянию объекта угрозы	• хранения данных • передачи данных • обработки данных

Приведенная классификация информационных угроз применима и для других объектов защиты, так как она позволяет адекватно дифференцировать по этим объектам сами угрозы и их источники.

В классификации угроз безопасности информации по субъектам — источникам они могут подразделяться на три группы: антропогенные, техногенные и стихийные.

Группа антропогенных источников угроз представляется:

• криминальными структурами, рецидивистами и потенциальными преступниками;

• недобросовестными партнерами и конкурентами;

• персоналом предприятия.

В свою очередь, злоумышленные действия персонала предприятия можно разделить на четыре категории:

1) прерывание — прекращение обработки информации, например, вследствие разрушения вычислительных средств. Такого рода действия могут иметь серьезные последствия для безопасности деятельности предприятия, даже если информация не подвергнется серьезным искажениям;

2) кража — чтение или копирование информации, хищение носителей информации с целью получения данных, которые могут быть использованы против интересов владельца (собственника) информации;

3) модификация информации — внесение в данные несанкционированных изменений, направленных на причинение ущерба владельцу (собственнику) информации;

4) разрушение данных — необратимое изменение информации, приводящее к невозможности ее использования.

К техногенным источникам угроз относятся некачественные технические и программные средства обработки информации, средства связи, охраны, сигнализации, другие технические средства, применяемые в учреждении, а также глобальные техногенные угрозы (опасные производства, сети энерго-, водоснабжения, транспорт).

Классификационный признак «по направлению» аналогичен признаку «по объекту посягательства». Признак «по степени опасности» дублирует признак «по величине ущерба». Анализируя приведенные классификации, следует признать следующие классификационные признаки и виды угроз [17] (таблица 1.3.):

Таблица 1.3.

Классификация угроз

Признаки	Угрозы
1. По месту возникновения	Внутренние, внешние.
2. По степени опасности	Особенно опасные, опасные.
3. По возможности осуществления	Реальные, потенциальные.
4. По масштабу осуществления	Локальные, общесистемные.
5. По длительности действия	Временные, постоянные.
6. По направлению	Производственные, финансовые, технологические, социально-экономические, эколого-экономические.
7. По отношению к ним	Объективные, субъективные.
8. По характеру направления	Прямые, косвенные
9.По вероятности наступления	Явные, латентные
10. По природе возникновения	Политические, криминальные, конкурентные, контрагентские и др.

Так, основные классификационные составляющие (признаки) угроз можно отобразить осями трехмерного пространства: X — виды угроз безопасности, Y — объекты защиты, Z — средства и методы защиты. Откладывая на каждой из осей максимальное на данный период число позиций, определенных по экспертным оценкам (или из теоретических, прогнозных, аналитических значений), получим ограниченную область (объем) потребностей безопасности («кубик безопасности»). Координате каждой точки этой области могут быть сопоставлены соответствующие формализованные особенности конкретного подлежащего защите объекта и выбраны те составляющие, которые и определят структуру потребностей

безопасности этого объекта, а, следовательно, и структуру службы безопасности, обслуживающей эти потребности [17].

К безопасности постоянно выдвигаются новые требования, а, значит, констатируются и новые угрозы, которые ранее, скорее всего, тоже имели место, но их не считали нужным учитывать. Поэтому к безопасности бизнеса некорректно относиться как к застывшему раз и навсегда определенному явлению. То состояние, которое фиксируется в концепциях безопасности, выступает неким эталоном, к которому предприятие стремится. Как только оно достигнуто или по мере изменения стратегических целей, руководство предприятия начинает ощущать необходимость в разработке новой концепции безопасности или совершенствовании существующей.

Такая управленческая интуиция имеет разумное основание. Сейчас много говорится о том, что будущее за адаптивными организациями, которые умеют быть гибкими, мобильными, затрачивать минимальное количество времени на выявление изменений в своем окружении, оценку их важности и оптимальную перестройку своей внутренней среды. Сохранять статичность при динамично развивающейся внешней среде, во-первых, трудно, во-вторых, неполезно. Кроме того, надо подчеркнуть, что современное предприятие – это не армия, не преступная группировка, чтобы с кем-либо воевать, бороться и т.п. Принятые в теории менеджмента термины военного происхождения не должны сбивать с толку. Речь там идет об адаптации за счет максимально эффективного использования своих возможностей в рамках принятой деловой культуры. Следовательно, есть смысл в делении всех угроз безопасности современного бизнеса на частично поддающиеся нейтрализации и не поддающиеся нейтрализации. Говорить о наличии угроз, в полной мере поддающихся нейтрализации, бессмысленно. Это будут уже не угрозы.

Любому предприятию в целях его успешного функционирования может понадобиться сохранить себя как целое, а также свои составляющие – персонал, информацию, материальные и нематериальные активы, финансы,

клиентуру и, кроме того, такое трудно детерминируемое явление, как перспективы развития. Эту разбивку можно считать структурой безопасности современного бизнеса. Соответственно, возможные угрозы:

– предприятию как целому – финансовая несостоятельность или некомпетентный менеджмент или порча репутации (ведущие к несостоятельности);

– от персонала – увольнение по собственному желанию или выбытие из-за смерти;

– информации – утечка стратегически важных сведений;

– материальным активам – физическое исчезновение (уничтожение или пропажа) или порча;

– нематериальным активам – их ликвидация (к примеру, отзыв лицензии, непродление сертификата и пр.);

– финансам – пропажа;

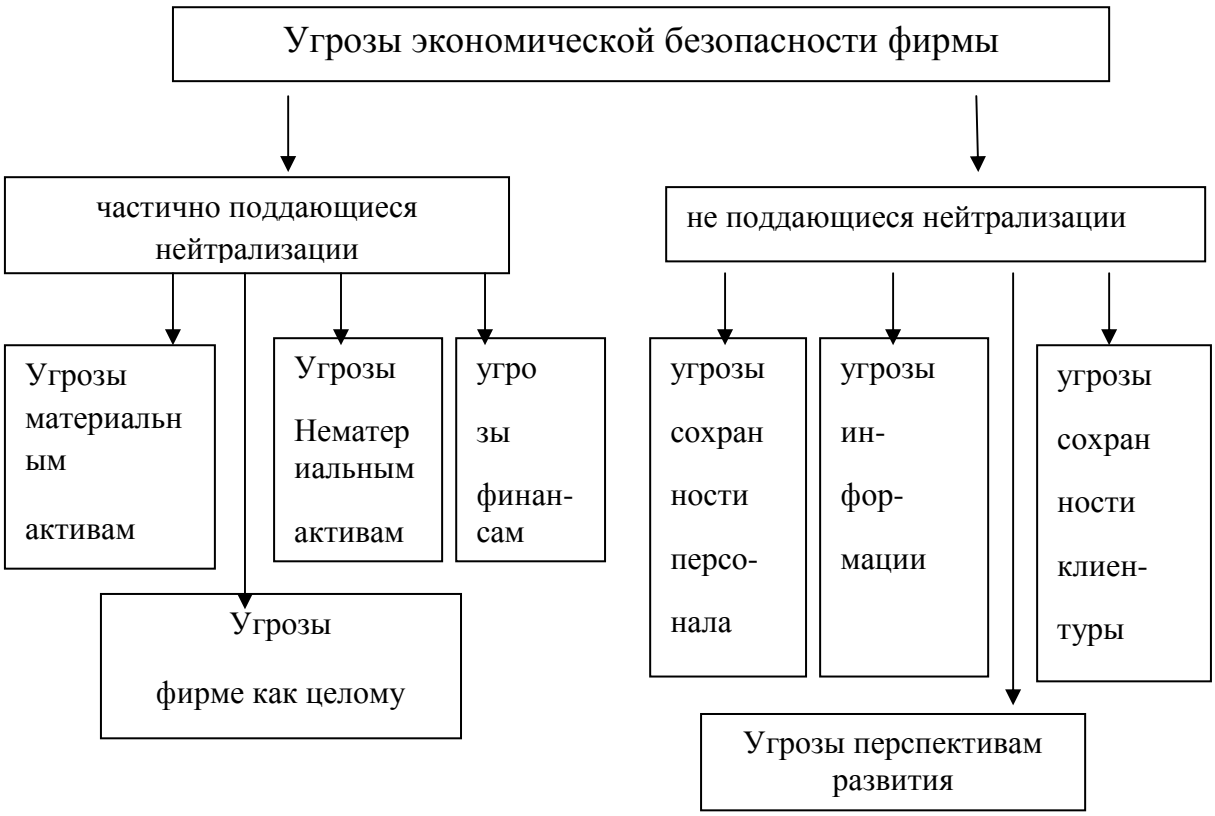
– от клиентуры – ее уменьшение не столько по количеству, сколько с точки зрения отдачи;

– перспективам развития – неблагоприятная рыночная конъюнктура.

Разумеется, указанные угрозы не являются взаимоисключающими, а пересекаются друг с другом. Любая классификация в определенной мере условна (рисунок 1.1.).

Рисунок 1.1.

Классификация угроз экономической безопасности фирмы



Таким образом, на современном этапе общественного развития:

- безопасность бизнеса целесообразно понимать не только как желаемое состояние защищенности от признанных негативными факторов внешней и внутренней среды, но и как процесс адаптации, который постоянно идет внутри бизнеса и подлежит управлению;

– указанный процесс связан с необходимостью адаптации предприятия к двум классам угроз: частично поддающимся нейтрализации и не поддающимся нейтрализации;

– структура рассматриваемой в таком свете безопасности предприятия включает сохранение себя (предприятия) как целого, а также своих

составляющих – персонала, информации, материальных и нематериальных активов, финансов, клиентуры и, кроме того, своих перспектив развития;

– в класс частично поддающихся угроз нейтрализации входят угрозы предприятию как целому, а также его материальным и нематериальным активам и финансам. К классу не поддающихся нейтрализации относятся угрозы сохранению персонала, информации, клиентуры и перспектив развития бизнеса.

1.2. Безопасность бизнеса как сложный феномен и многоуровневая система

Известно, что экономическое благополучие и могущество любого бизнеса держится на трех составляющих, имя которым – развитие, безопасность и прибыль.

Основные проблемы безопасности отечественного бизнеса заключаются в следующем. Во-первых, рыночная экономика, построенная на конкуренции, очень динамичная система, а, следовательно, и очень рискованная. Во-вторых, отечественный рынок находится в стадии становления, и поэтому многие механизмы еще просто не отработаны. В-третьих, у нас пока отсутствуют устойчивые нормы права защиты интересов предпринимателей.

Безопасность бизнеса – это состояние защищенности его жизненно важных и законных интересов от внешних и внутренних угроз в различных противоправных формах, обеспечивающее его стабильное развитие в соответствии с уставными целями. Защищенность правовых, экономических и производственных отношений, материальных, интеллектуальных и информационных ресурсов составляет сущность безопасности бизнеса. Безопасность предприятия – это такое состояние его правовых экономических и производственных отношений, а также материальных, интел-

лектуальных и информационных ресурсов, которое выражает способность предприятия к стабильному функционированию [29,3].

Обеспечение безопасности бизнеса представляет собой комплекс организационно-правовых, социально-экономических, технико-технологических и административных мер.

Безопасность предприятия зависит от разных причин. В частности, ущерб интересам предпринимателя может быть нанесен в результате недобросовестных действий конкурентов, невыполнения партнерами, заказчиками, поставщиками, клиентами своих обязательств по оплате контрактов, поставке товаров и т. п., а также кризисных явлений в экономике, непредсказуемых изменений конъюнктуры рынка, стихийных бедствий, чрезвычайных происшествий, управленческой некомпетентности, социальной напряженности и, наконец, неблагоприятной экономической политики государства.

Таким образом, факторы, влияющие на уровень безопасности предприятия, могут быть внутренними и внешними, экономическими и внеэкономическими, объективными и субъективными. Если исходить из того, что главный принцип рыночной экономики это взаимодействие хозяйствующего объекта и рынка, который представляет собой совокупность хозяйствующих субъектов и вместе с тем самостоятельную целостность, то хозяйствующий субъект может существовать только при условии бесперебойного взаимодействия с рыночной средой. Для этого необходимо нормальное функционирование, как самого предприятия, так и рынка в целом.

Сегодня эффективная безопасность бизнес деятельности представляется как система мер, которая обеспечивается на следующих взаимосвязанных направлениях: защита от преступного мира; защита от нарушений закона с тем, чтобы самим не попасть под санкции; защита от

недобросовестной конкуренции; защита от противоправных действий собственных сотрудников.

Эти направления деятельности реализуются на следующих участках: производственный (сохранность материальных ценностей); коммерческий (оценка партнеров, юридическая защита интересов); информационный (определение значимости информации, порядка поступления, пользования, передачи, защиты от хищения); кадрового обеспечения.

Безопасность современного бизнеса обеспечивается с помощью следующих режимов: конфиденциальности и защиты объектов интеллектуальной собственности, что составляет информационную безопасность; физической охраны, то есть обеспечение физической безопасности имущества и персонала предприятия.

Защитные меры, обеспечивающие экономическую безопасность предпринимательства, можно рассматривать как объектовые, групповые и индивидуальные, а по характеру – активные и пассивные средства и мероприятия.

Обеспечение экономической безопасности бизнеса можно классифицировать следующим образом: по целям действий – предупреждение, выявление, обнаружение, пресечение и ликвидация последствий; по направлениям обеспечения – правовая, организационная и инженерно-техническая защита; по видам угроз – разглашение, утечка, несанкционированный доступ; по объектам – территория, здания, помещения, аппаратура; по уровням охвата — объектовая, групповая, индивидуальная; по видам объектов – персонал, материальные и финансовые ценности, информация; по характеру – активные и пассивные. В предпринимательской среде следует разграничивать сформированные группы и объединения по принципу их защищенности.

Однако главным в безопасности предпринимательства являются экономические рычаги по возмещению ущерба и предотвращению негативных последствий для организации бизнеса. В этом заключается основной смысл обеспечения экономической безопасности предпринимательства от противоправных действий. А если так, то поддержание правопорядка в экономической сфере заключается в развитии судебной системы с ведущей ролью арбитражных судов. Только арбитражные суды, а не административные и другие внешнеэкономические меры могут создать нормальный правопорядок в экономике и сделать предпринимательство цивилизованным.

Основой экономического развития любого предприятия является научно-технический прогресс и его способность осуществлять плавный переход к передовым технологиям. В этой связи можно утверждать, что стержнем экономической безопасности в современных условиях являются технико-экономическая независимость хозяйствующего субъекта и его технико-экономическая неуязвимость. В этой связи основным содержанием деятельности службы безопасности предприятия являются следующие функциональные направления:

1. Своевременное выявление угроз жизненно важным интересам предприятия. При этом основными методами получения информации являются деловая разведка и прогноз-анализ.

2. Предупреждение проникновения (агентурного и технического) к конфиденциальным сведениям (коммерческой тайне) предприятия и обеспечение сохранности информационных ресурсов предприятия. Главными средствами при этом являются: соблюдение охранно-пропускного режима, бдительность сотрудников и технические средства защиты.

3. Обеспечение физической охраны руководства и сотрудников предприятия. При этом основными средствами и методами являются:

организация системы упреждающих мер, профессионализм охраняющих и дисциплина охраняемого лица.

Следует упомянуть, что, как свидетельствует практика, при обеспечении экономической безопасности не всегда занимает полагающееся ей место защита интеллектуальной собственности предприятия. Кража интеллектуальной собственности может быть в сотни раз серьезнее материальной. Предприятие, лишившееся ее, рискует потерять свое место в конкурентной борьбе и будет вынуждено сократить штат служащих, отказаться от планов развертывания производства. Все это может уменьшить его дивиденды и, в конце концов, привести к банкротству.

Очевидно, что сегодня отечественные предприниматели начинают понимать, что коммерческая тайна является обязательной для обеспечения безопасности предприятия. Известно, что один из самых распространенных путей утечки информации — небрежное обращение со служебными документами. Как правило, огромное количество входящих и исходящих документов в немалой степени затрудняет контроль за их сохранностью. Особо следует отметить, что большие возможности для незаконного распространения деловой информации представляет современная фотокопировальная техника. Существенный ущерб несут предприятия и от утечки информации в результате подслушивания конкурентами телефонных разговоров, а также регистрации излучений компьютерных терминалов. По мнению специалистов, несмотря на самые совершенные технические средства, наилучшей защитой от промышленного (коммерческого) шпионажа является поддержание порядка и соответствующего режима секретности внутри предприятия.

Существуют шесть принципов эффективной защиты информации:

1. Ограничение доступа к коммерческой тайне (списки участников совещания, рассылки, предупреждение сотрудников о характере и степени важности информации).

2. Защита всех элементов проекта, являющегося коммерческой тайной. При этом следует избегать защитных мер, которые автоматически привлекают внимание. Следует учредить достаточно эффективную общую систему, ограничив число мер частного характера.

3. Фрагментация информации с целью ограничения ее значимости. Обобщающие документы следует составлять как можно позже и только в тех случаях, когда это необходимо. Когда такой документ составляется, необходимо: применять особые меры защиты, существующие для документов с грифом «весьма конфиденциально»; когда это, возможно, знакомить сотрудников лишь с отдельными фрагментами такого документа (по принципу служебной необходимости); включать в документ лишь сведения, совершенно необходимые тому, кому они предназначаются; использовать кодовые обозначения (условные наименования) для всех важных проектов, в том числе и для несекретных.

4. Назначение ответственных работников за документы, содержащие коммерческую тайну.

5. Принятие самых простых решений, которые чаще всего оказываются самыми эффективными.

6. Разработка комплексных систем защиты, обеспечивающих непрерывность действия системы [22], [23].

Трудность обеспечения экономической безопасности любого предприятия заключается в том, что внутри самой предпринимательской структуры очень часто действуют скрытые от глаз противоречивые, если не

взаимоисключающие, групповые и личные интересы. В связи с этим проблема службы экономической безопасности предприятия заключается в том, чтобы найти такие сферы, которые были бы выгодны (приемлемы) всем субъектам экономической деятельности фирмы в равной мере. Сгладить их, не разобравшись в существе, для субъектов обеспечения безопасности представляется затруднительным.

С позиции системного подхода безопасность бизнеса должна соответствовать следующим принципам:

- непрерывность - осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности организации. При этом руководители организаций должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала;

- комплексность - использование всех средств защиты финансовых, материальных, информационных и человеческих ресурсов во всех структурных подразделениях организации и на всех этапах ее деятельности. При этом комплексность реализуется через совокупность правовых, организационных и инженерно-технических мероприятий без их приоритетного выделения;

- своевременность - обеспечение безопасности с использованием упреждающих мер. При этом принцип своевременности предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности, а также разработку эффективных мер предупреждения посягательств на интересы организации;

- законность - обеспечение безопасности на основе законодательства АР и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции. При этом необходимо иметь в виду, что вопрос дозволенности тех или иных методов обнаружения и пресечения

правонарушений в рамках действующего законодательства и большого количества ведомственных подзаконных актов в настоящее время в большинстве случаев остается открытым;

- активность - обеспечение безопасности организации с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств;

- универсальность - обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения;

- экономическая целесообразность - сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности должна не превышать размера возможного ущерба от любых видов риска;

- конкретность и надежность - определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом обязательным является достаточное дублирование методов, средств и форм защиты при обеспечении безопасности организации;

- профессионализм - реализация мер безопасности должна осуществляться только профессионально подготовленными специалистами. При этом в условиях быстрого развития средств и систем безопасности необходимо постоянное совершенствование мер и средств защиты на базе обучения личного состава;

- взаимодействие и координация - осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц. При этом вопрос о взаимодействии и координации касается не только подразделений и лиц, непосредственно отвечающих за безопасность, но и их связи с остальными подразделениями организации;

- централизация управления и автономность - обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности организации в целом.

1.3. Зарубежные модели обеспечения безопасности бизнеса

В создании частных служб безопасности в Азербайджане достаточно широко используется мировой опыт. Однако в разработках правового обеспечения деятельности частных структур пока еще есть существенное отставание как в обеспечении собственной их деятельности, регламентации прав и обязанностей, так и в смежных областях — по защите коммерческой тайны и конфиденциальной информации, борьбе с компьютерными преступлениями.

Отечественное законодательство находится в начальной стадии формирования правового поля частной деятельности по вопросам безопасности. Например, в США только вопросы защиты информации обеспечены более чем 500 законами. По данным Национального института юстиции США, в стране насчитывается более 1,5 млн. частных охранников (втрое больше, чем сотрудников полиции). За последние 20 лет численность персонала частных охранных структур выросла на 64% [36].

Сегодня прослеживается явное противоречие между попыткой регламентировать частную деятельность служб безопасности и реальными потребностями рынка в этой области: ни в коем случае не допустить конкуренции частных структур с государственными правоохранительными органами, а это не учет основной тенденции, сложившейся во всем мире, — существенный рост доли и влияния частных структур в обеспечении безопасности бизнеса.

Опыт работы фирм, занимающихся обеспечением безопасности, показывает, что со стороны отечественных предпринимателей сегодня

предъявляется спрос в основном на определенные виды услуг и чаще всего — на физическую охрану зданий, инкассацию, комплекс защитных мер от рейдерства и прослушивания телефонных каналов связи, помещений от радиозакладок, компьютеров и компьютерных сетей от проникновения и вирусов. Сегодня в Азербайджане функционирует множество фирм, осуществляющих безопасность бизнеса. Например, POSTECH ISS, Seotech , Azerms LLC, Gesco General Security. Например, компания "POSTECH Security Systems" на сегодняшний день является одним из крупнейших операторов рынка систем безопасности и видеонаблюдения, завоевавшим репутацию надежного делового партнера и постоянно работающего над повышением качества и эффективности собственной работы. А компания Gesco General Security осуществляет охрану нефтяных компаний, крупных объектов, жилых домов, офисов, банков, строительных участков и других объектов; определяет местонахождения и слежение в реальном времени за движимым имуществом при помощи глобальной спутниковой системы навигации и позиционирования GPS + GSM; обеспечение пропускного и внутриобъектных режимов на охраняемых объектах; обеспечение личной безопасности физического лица и его сопровождение на автомобиле; обеспечение безопасности и поддержание порядка при проведении массовых мероприятий [39].

Совсем редко исследуется, с точки зрения безопасности, проблема внешних контактов фирмы. Здесь предполагается анализ репутации соисполнителей, контрагентов, их кредитоспособности, финансовой состоятельности; изучение конкурентов, исследование рынка, т. е. обеспечение прикладных аспектов безопасности современного маркетинга.

Проведенный нами анализ зарубежной организации безопасности бизнеса показывает, что в развитых странах к настоящему времени сложились следующие две основные тенденции:

1) расширение и активизация деятельности службы безопасности в промышленных и финансовых фирмах. Создание частных служб безопасности отражает потребности деловых кругов в уменьшении коммерческих рисков и повышении безопасности предпринимательской деятельности;

2) постепенный переход от ориентации на физическую охрану к использованию специальных средств защиты и сигнализации, которые либо сами нейтрализуют угрозу, либо оповещают полицию и службу безопасности. Идеальный вариант — автономная система защиты, управляемая несколькими операторами, которая сама оценивает степень угрозы и может дать сигнал тревоги без их участия. Эта тенденция обусловлена высокой стоимостью физической охраны.

Поэтому службы безопасности крупных корпораций ведут обширные электронные картотеки и досье на национальные и зарубежные фирмы-партнеры, фирмы-конкуренты, а также на работающих в них сотрудников. Там отражены сведения о структуре, организационных особенностях, характеристиках готовой продукции конкурентов, применяемых ими технологиях, недостатках в работе персонала и подборе кадров. В последние годы в некоторых странах для обработки этих данных созданы специальные крупномасштабные информационно-поисковые системы.

Развитие сети охранных компаний позволяет экономить государственные расходы на содержание полиции и других спецслужб. Эта тенденция в развитых странах носит уже общенациональный характер.

Если конкретизировать основные задачи, решаемые сегодня в различных странах службами безопасности, то можно отметить, что их характер зависит от национальных условий, исторической традиции, уровня развития экономики, влияния деятельности спецслужб на государственные

институты. Но поскольку в основе деятельности службы безопасности в любой стране с рыночной экономикой лежит задача защиты от экономических рисков, то основные направления деятельности служб безопасности схожи.

Рассмотрим рынок услуг безопасности бизнеса в США, Франции, Германии и Японии.

С начала 1990-х гг. США приступили к внедрению широкомасштабной системы коллективной безопасности американского бизнеса. Так, Государственный департамент, головная организация — консультативный совет по обеспечению безопасности за рубежом, более 500 корпораций США регулярно обмениваются информацией через по наиболее актуальным вопросам национальной и экономической безопасности.

В США сложились три основных типа частных правоохранительных организаций: охранные агентства; сыскные бюро; службы безопасности в различных промышленных и коммерческих структурах [36].

Анализируя рынок услуг безопасности во Франции, можно отметить некоторые отличительные направления деятельности частных служб, такие как борьба со злоупотреблением торговой маркой, выявление недобросовестной конкуренции, промышленный шпионаж и контршпионаж, обеспечение мер безопасности в банковской системе. Особый интерес представляет используемая промышленными службами безопасности система проверки персонала. В частности, трехступенчатые проверки позволяют предупредить реальные и потенциальные угрозы безопасности объекта при условии регулярности и тщательности этих проверок, а также при контроле над увольняемым персоналом. Особое внимание французскими специалистами уделяется информационной безопасности за счет предупреждения компьютерных преступлений. Комплекс мер информационной безопасности включает охрану рабочих помещений, в первую очередь — аппаратного зала. Обя-

зательно применение семизначных программных паролей и их замена после увольнения служащих. Ограничен доступ персонала к терминалам, имеющим выход на особо важные информационные файлы. Контролируется поведение персонала. Поскольку большинство компьютерных преступлений совершают сотрудники фирм, проверяются их деловые операции и личные счета.

Французские службы безопасности активно используют для сбора информации о своих партнерах методы анкетирования, интервью, опросные листы, выведывание и "выспрашивание", визуальное наблюдение с использованием технических средств. Технические средства они применяют также для подслушивания телефонных переговоров, перехвата телексов и телеграфной переписки, скрытого фотографирования, внедрения в рабочие помещения подслушивающих устройств [36].

Полученные оперативные сведения фирмы используют для заблаговременного выявления тактики конкурентов на переговорах, уровня их цен и объемов финансирования тех или иных проектов, прогнозирования кадровых перестановок, оценки экономического состояния интересуемого объекта. Высокий уровень технической оснащенности позволяет службам безопасности систематически выявлять акты промышленного шпионажа в отношении компаний — иностранных конкурентов французских фирм.

В Германии охрана, безопасность, защита и частные расследования — предмет деятельности свыше тысячи частных фирм, число занятых в которых составляет около 130 тыс. человек. Из них 63% заняты в сфере охраны производственных и служебных помещений. Расходы на обеспечение безопасности в этой стране 10 млрд. евро. В среднем каждая немецкая семья тратит на защиту собственности 400 марок. Эти расходы непрерывно растут.

Производство средств обеспечения безопасности является весьма прибыльным. Ситуация в промышленности, производящей средства

обеспечения безопасности, относительно стабильна, несмотря на то что у крупных фирм объем производства растет всего на 1-2%, а в мелких фирмах, производящих оригинальные системы и компоненты, — до 15% [36].

Для Германии характерно использование частных служб безопасности по заказам германских торгово-промышленных и посреднических фирм.

В последние годы руководство МВД и БФФ (контрразведка) Германии выступили с инициативой усилить административно-техническую помощь частным детективным и охранным агентствам, которым отводится роль вспомогательных подразделений секретных служб. С начала 90-х гг. в этой стране постоянно увеличиваются масштабы профилактических акций, усиливается безопасность в банковской сфере. Так, совместным совещанием Центробанка и спецслужб рекомендовано банкам сократить на 50% штаты сотрудников, которым разрешены контакты с иностранцами. С тех пор служащих банков, состоящих на учете спецслужб, систематически проверяют. К финансовым операциям с иностранцами допускаются в присутствии одного из руководителей банка только служащие, прошедшие специальную подготовку. Кроме того, в объединенную информационную систему полиции и спецслужб вводятся сведения обо всех иностранных посетителях, запрашивавших у банка информацию о клиентах или фирмах. Рядовым клиентам банков предоставляется лишь обобщенная банковская статистика и информация, не раскрывающая специфику и конъюнктуру денежного рынка в стране [28].

Экспертами отмечается интенсивное развитие в течение последнего десятилетия частных служб безопасности Японии. Там действуют более тысячи частных служб безопасности, сосредоточенных преимущественно в крупных городах. Основные услуги, которые они оказывают, имеют свои отличительные от других стран особенности: оценка кредитоспособности отдельных фирм и граждан; сбор сведений о лицах, поступающих на работу в местные фирмы и банки; получение и накопление сведений о потенциальных

клиентах; исследование национального рынка и зарубежных рынков товаров и услуг; обеспечение конфиденциальной информацией участников деловых переговоров; сбор доказательств в интересах клиентов и адвокатов по гражданским делам. Эксперты отмечают ряд недостатков в деятельности этих частных структур. К ним относится возможность несанкционированного доступа к национальному полицейскому компьютеру, а также распространенная практика сговора с сотрудниками полиции с использованием их в корыстных целях.

В связи с ростом экономических преступлений службы безопасности Японии уделяют повышенное внимание разработке теории и совершенствованию практики "комплексной защиты". Такой подход, получивший название корпоративной защиты, подразумевает реализацию особой системы мероприятий. Корпоративная защита обеспечивает эффективный контроль над всей деятельностью предприятия, начиная от деловых связей с партнерами и вплоть до проверки персонала, защиту от промышленного шпионажа и мошенничества со стороны своих сотрудников, партнеров по бизнесу. Мероприятия корпоративной защиты обеспечивают также конфиденциальность информации о планируемых и принимаемых решениях правлением предприятия; планирование и проведение регулярных проверок рабочих и служащих. Особое значение придается выработке планов работы в кризисных ситуациях. Эти планы регламентируют действия персонала по выходу из различных типовых инцидентов и чрезвычайных обстоятельств (пожары, наводнения, угрозы взрывов, похищений, шантаж, вымогательство, шпионаж, вредительство, диверсионно-террористические акты и т. п.). Специальные противодиверсионные программы, также входящие в корпоративный комплекс мер, предусматривают: внедрение специальных методов управления и проведение кадровой политики с учетом рисков кризисных ситуаций; сбор службой безопасности данных о возможных

террористических угрозах; отработку тактики деятельности сотрудников службы безопасности в чрезвычайной ситуации; обеспечение безопасности функционирования оборудования предприятия. Для разработки механизма управления в кризисных ситуациях формируются специальные комитеты в составе главного исполнительного директора фирмы, вице-президента, руководителей финансового и юридического отделов, службы кадров, отдела по связям с общественностью и руководителя службы безопасности фирмы [36].

Особое место в обеспечении безопасности японских фирм занимает проведение разведывательно-информационной деятельности. Она заключается в создании информационной базы данных по определенной тематике за счет обработки официальных источников и накопления сведений, полученных от контактов и связей из числа местных граждан. Аналитическая обработка этих информационных массивов с учетом оперативной информации позволяет оценить стабильность политической обстановки в определенном регионе или стране и вероятность непосредственной угрозы для корпорации.

В современных условиях роста внешних и внутренних угроз, экономического кризиса и жесткой конкуренции на международном рынке владельцы и руководители компаний ищут эффективные и экономичные способы обеспечения безопасности. Многие видят решение проблемы в аутсорсинге.

Бизнес-модель, получившая название «аутсорсинг безопасности», уже довольно давно применяется в мировой практике. Главными причинами обращения к этой модели эксперты считают необходимость повышения уровня безопасности компании при одновременном снижении затрат и стремление сосредоточиться на основной деятельности.

По данным проведенного в Британии исследования, британский рынок услуг аутсорсинга в сфере безопасности в 2012 году составил 5 млрд фунтов стерлингов и продолжает расти вопреки экономическому кризису.

Значительная часть рынка приходится на долю частных охранных фирм. Это наиболее традиционная сфера применения аутсорсинга не только в Британии, но и в большинстве других стран [37].

Многие владельцы и руководители предприятий считают нерентабельным содержание собственной службы охраны, особенно учитывая, что для работы с современными техническими средствами требуются профессионалы с хорошей подготовкой и опытом работы. Поэтому услуги частных охранных агентств становятся все более востребованными. Это позволило таким фирмам, как Andrews International, Garda,Allied Barton стать крупными игроками на международном рынке.

В частности, американская компания Andrews International предлагает услуги вооруженной и невооруженной охраны на территории США, Канады, Мексики и Индии. Более 15 000 сотрудников фирмы, охраняющих частные и государственные объекты, прошли тщательный отбор и подготовку. Для каждого объекта фирма разрабатывает специальную программу по организации охраны и проводит набор сотрудников среди местного населения, которые затем проходят курс подготовки с учетом местных требований и особенностей объекта. При отборе кандидатов используется разработанная Andrews International методика, позволяющая не только оценить профессиональный уровень кандидата, но и составить его психологический портрет, чтобы личностные характеристики и жизненные ценности сотрудника охраны соответствовали философии и ожиданиям компании, в которой ему предстоит работать. Программа также предусматривает постоянный Контроль, оценку работы сотрудников и их переподготовку в дальнейшем [37].

Относительно новое явление — аутсорсинг в области управления службами безопасности. Во многих крупных международных компаниях руководители департаментов безопасности состоят в штате консалтинговых фирм-аутсорсеров и выполняют функции консультантов и одновременно менеджеров. Эта схема особенно удобна, если крупной компании требуется

дополнительный руководитель службы безопасности под конкретный проект. Таких специалистов предлагают, например, агентства Securitas Security Servicesи Control Risks Group [38].

Аутсорсинг находит применение и в сфере монтажа систем безопасности. Несмотря на то, что многие компании предпочитают выполнять установку оборудования силами собственных специалистов, существует множество фирм, предлагающих профессиональные услуги в этой области. Чаще всего их клиентами становятся крупные государственные подрядчики, так как сами они не имеют достаточного количества специалистов для выполнения монтажных работ по всем проектам.

Распространенным явлением за рубежом является и аутсорсинг части работ по установке систем безопасности — например, монтажа высоковольтного оборудования. В США такие услуги предлагает компания Outsource Telecom, которая может предоставить специалистов по монтажу систем охранной и пожарной сигнализации, CCTV и контроля доступа; монтажников электропроводки,имеющих опыт работы с оборудованием изготовителей AMAG, Lenel, Panasonic, Bosch, Honeywell, Dedicated Micros, Carrier, HID, Johnson Controls, Pelco. Компания предлагает нескольких кандидатов в соответствии с требованиями заказчика, из которых заказчик затем выбирает лучшего. Возможно предоставление сотрудников на контрактной основе на срок до 6 месяцев или на постоянной основе. В последнем случае заказчик оплачивает до 20 % заработной платы сотрудника [38].

Пользуясь тем, что многие крупные поставщики систем безопасности все чаще отдают на аутсорсинг монтаж и обслуживание оборудования, другая американская компания — FCIAssociates успешно выполняет эти работы и уже осуществила около 600 000 проектов более чем в 1 000 городов США. Среди ее клиентов — такие известные в отрасли фирмы, как ADT Security Services, Checkpoint Security, Honeywell, Johnson Control и UTC [38].

Многие годы аутсорсинг успешно используется в сфере мониторинга электронных систем безопасности. Поставщики оборудования считают экономически выгодной передачу мониторинга своих систем аутсорсерам, которые, как правило, имеют все необходимые сертификаты и разрешения. Это позволяет поставщикам сосредоточиться на продажах, монтаже оборудования и не потерять важные контракты.

Одной из самых быстро развивающихся форм аутсорсинга является облачное видеонаблюдение. Агентство IMS Research прогнозировала, что мировой рынок «видеонаблюдения как услуги» (VSaaS) к 2014 году превысит миллиард долларов, то есть вырастет вдвое по сравнению с 2011годом. Прогнозы оправдались. По мнению аналитиков, VSaaS представляет интерес для очень широкой категории заказчиков — от частных пользователей и малого бизнеса до крупных организаций и государственных учреждений [38].

Для того чтобы контролировать многочисленные электронные системы сигнализации, автоматизации и энергопотребления с удаленной станции, смартфона или через web-браузер, требуется доступ к скоростному Интернету,сотовой связи и Wi-Fi. Это позволяет телекоммуникационным компаниям объединять такие сервисы с услугами связи и продавать пакетные предложения по более низким ценам. Их клиентами в первую очередь становятся предприятия малого бизнеса.

Зарубежные аналитики констатируют, что аутсорсинг затронул и такие сферы, как проектирование систем безопасности, управление проектами и даже продажа оборудования. Компания-аутсорсер полностью берет на себя все заботы по обеспечению безопасности на объекте заказчика. Однако многих волнует вопрос о том, до какой степени разумно доверять свою безопасность сторонней компании. Главным критерием здесь должно быть сохранение контроля, координации и качества услуг. Главными условиями успешного применения аутсорсинга являются анализ экономической целесообразности; оценка рисков и уязвимых мест; тщательная проработка с

поставщиком услуг соглашения, определяющего взаимную ответственность сторон. Обычно в зарубежной практике в этом процессе принимают участие представители клиента и аутсорсера, а также независимые эксперты и юристы. Соглашение должно предусматривать механизмы контроля; решения спорных вопросов и изменений требований; инструменты, необходимые для эффективного управления процессом оказания услуг.

Международный опыт показывает, что аутсорсинг является гибким инструментом, позволяющим снизить операционные расходы и риски, связанные с непрофильной деятельностью, использовать передовые технологии и ранее недоступные ресурсы. Это способствует повышению конкурентоспособности компании. Тем не менее, к разработке стратегии аутсорсинга следует подходить с осторожностью, учитывая преимущества и оценивая возможные риски. При принятии решения о том, в какой степени для работы службы безопасности будут использоваться внешние ресурсы, руководству компании важно не утратить контроля и не допустить, чтобы экономическая выгода привела к снижению уровня безопасности.

Таким образом, проведенный анализ показывает не только рост потребностей рынка услуг в сфере безопасности, но и широкое влияние частных служб безопасности на различные аспекты деятельности промышленных предприятий, фирм, финансовых структур. Последнее, в свою очередь, обусловливает возрастание их роли и дает им право претендовать на самостоятельное и весьма важное место в системе обеспечения национальной безопасности страны в целом.

ГЛАВА II. Анализ проблем обеспечения безопасности кредитно-финансовой организации на примере «ОАО Банк ВТБ (Азербайджан)»

2.1. Анализ возможных угроз безопасности банка

Открытое Акционерное Общество Банк ВТБ (Азербайджан) — универсальный банк, предоставляющий комплекс современных продуктов и услуг международного уровня. ОАО Банк ВТБ (Азербайджан) является дочерним банком ОАО Банк ВТБ. ОАО Банк ВТБ имеет наивысший для российских банков рейтинг международных рейтинговых агентств Moody`s Investors Service, Standard & Poor`s и Fitch.

Акционерный капитал ОАО Банк ВТБ (Азербайджан) разделен между российской стороной - ОАО Банк ВТБ (51% акций) и азербайджанской – ОАО «AtaHolding» (48.99%) и частным лицом (0.01%).

Официальное открытие Банка ВТБ (Азербайджан) состоялось 23 ноября 2009 года. Банковская лицензия №162 была выдана Центральным Банком Азербайджанской Республики 11 марта 2009 года [34].

Банк ВТБ (Азербайджан) оказывает широкий спектр услуг клиентам. В перечень услуг ВТБ (Азербайджан) входят и небанковские финансовые услуги – трастовые и инвестиционные, лизинг и другие услуги, которые оказываются через соответствующие дочерние компании Группы ВТБ.

Банк ВТБ (Азербайджан) входит в состав группы ВТБ, представленной банками и финансовыми организациями в странах СНГ, Европы, Азии и Африки.

Основными факторами конкурентоспособности банка являются:

- Сильная управленческая команда;
- Существенный в масштабах локального рынка клиентский портфель;

- Развитые компетенции в сфере обслуживания ключевых клиентских групп: крупных и средних корпоративных клиентов, премиального сегмента физических лиц, сотрудников корпоративных клиентов;
- Взвешенная политика регионального развития, обеспеченная эффективной системой управления издержками и высокой долей филиальной сети в бизнесе банка;
- Высокий рейтинг системы управления рисками;
- Относительно низкий уровень зависимости от международных финансовых рынков, диверсифицированная ресурсная база.

ОАО Банк ВТБ (Азербайджан) традиционно уделяет особое внимание поддержанию высокого качества активов, эффективному управлению рисками и издержками. Миссия и цели банка:

- Удобный сервис
- Гибкий подход
- Простые решения
- Уважительное отношение

Среднесрочная перспектива развития ОАО «Банк ВТБ (Азербайджан)» на период до 2016 г. основана на анализе опубликованных Центральном Банком Азербайджана “Основных положений проведения денежно кредитной политики”, индикативных показателях, представленных Министерством Экономического Развития Азербайджана.

В рамках стратегии развития на три года (2013-2015) Банк поставил перед собой следующие цели:

- открытие дополнительно 10-15 филиалов, из которых 3 не столичных филиала будут располагаться в некоторых крупных городах Азербайджана;

- завершение строительства центрального офиса Банка, отвечающего высоким стандартам качества и безопасности;
- создание сети банкоматов в количестве 50;
- рентабельность собственного капитала (ROE) Банка составит не менее 10%;
- совершенствование операционной деятельности с целью повышения качества обслуживания клиентов всех категорий;
- формирование такого имиджа Банка, который позволит ему в течении 3-х лет стать узнаваемым на банковском рынке и получить значимый общественный статус;
- формирование динамичной, высокообразованной и мотивированной команды.

Таблица 2.1.

Стратегии развития «ОАО Банк ВТБ (Азербайджан)» на 2013-2015 годы

годы / Показатель	**2013**	**2014**	**2015**
увеличение размера активов	150 млн.ман	200 млн. ман	250 млн.ман
увеличение кредитного портфеля	120 млн. ман	160 млн. ман	210 млн. ман

Источник: http://www.vtb.az

Для утверждения финансовой отчетности выбор внешнего аудита происходит на основе следующих принципов:

- Внешний аудит должен иметь высокий рейтинг или быть одним из 10 крупнейших международных аудиторских компаний, которая имеет специальное разрешение (лицензию);
- Услуги, предлагаемые аудиторской компании;
- Плата за услуги;

- Требования использование аудиторских отчетов.

Основываясь на этих принципах и требованиях получают предложения от внешних аудиторских фирм. Предложения, представленные внешней аудиторской компании изучаются, и отобранный пакет предложений представляется Аудиторским комитетом Наблюдательному совету.

Основываясь на протокол Наблюдательного совета, подписывается соглашения с выбранной внешней аудиторской компанией. На данный момент в качестве внешней аудиторской компании была выбрана "RSM Azerbaijan".

В Банке ВТБ (Азербайджан) разработана и действует Политика противодействия внутреннему мошенничеству, в которой изложена система мер по предупреждению, выявлению и реагированию на факты мошенничества и злоупотреблений. Также созданы внутренние инструкции работы сотрудника Банка именно в этой части. Указанные внутрибанковские документы обязательны для исполнения сотрудниками всех структурных подразделений.

Политика противодействия внутреннему мошенничеству устанавливает требования и правила поведения сотрудников, определяет перечень действий по предупреждению мошенничества.

Цель Политики противодействия мошенничеству - реализация эффективных мер по предотвращению мошенничества и злоупотреблений в банке, формирование культуры этики и высокой честности среди сотрудников.

Самый сложный для выявления вид мошенничества — это внутреннее мошенничество, осуществляемое с участием сотрудников, работающих в организации. Подобного рода мошеннические действия могут осуществляться в течение длительного промежутка времени и приводить к весьма серьёзным потерям для организации.

Классификация угроз имущественной безопасности (на примере банка):

- хищение денежных средств путем несанкционированного проникновения в компьютерные сети банка и перехвата управления финансовыми операциями;
- хищение денежных средств с использованием поддельных банковских карточек;
- хищение денежных средств с использованием поддельных платежных документов (поручений, сертификатов, чеков, векселей и т.п.);
- мошенничество при получении кредитов;
- хищение высоколиквидных активов банка (наличных денег, ценных бумаг, золота и т.п.) с использованием насильственных методов (ограбление);
- хищение высоколиквидных активов банка с использованием ненасильственных методов (кража);
- хищение или умышленная порча материальных активов банка.

Возможными субъектами угроз имущественной безопасности банка в современных условиях чаще всего являются индивидуально действующие злоумышленники (хакеры, мошенники, взломщики), нелояльные собственные служащие и, реже, преступные группировки. Распространенным и наиболее опасным явлением выступает преступный сговор между сотрудником банка и сторонними злоумышленниками.

Мошенник — это личность, для которой характерны жадность и лживость. Анализ показывает, что сотрудники, склонные к мошенничеству, работают годами и ничего подобного не совершают, пока не попадут в определенную ситуацию. В то же время средний период от момента совершения до момента выявления мошенничества составляет до 3 лет. Это дает основания для утверждения, что тот, кто совершает мошенничество по прошествии 5–10 лет, на момент поступления в компанию не имел такой установки. К такому решению подталкивают изменения в личных

обстоятельствах и иные критические ситуации в жизни работников. Они совершают злоупотребления, когда имеют должностные возможности и условия, располагают доверием коллег, понимают слабые стороны контроля. Также практика показывает, что причиной значительной части реализованных угроз безопасности работодателя со стороны собственных сотрудников является их неспособность противостоять воздействию со стороны третьих лиц. Эти лица, преследуя собственные интересы, склоняют сотрудников организации к различным формам нарушения доверия работодателя вплоть до прямых должностных преступлений (например, коррупция при выдаче кредита) [15].

Чаще всего объектами рассматриваемой угрозы являются должностные лица банка, рабочие места которых обеспечивают доступ к: - конфиденциальной информации; - управлению денежными средствами и иными ликвидными активами; - реализации функций управления, регулирования и надзора.

Предметная классификация угроз безопасности банка

а) По признаку целевой направленности угрозы выделяются:

- угроза разглашения конфиденциальной информации, которое может нанести банку ущерб в форме ухудшения его конкурентных позиций, имиджа, отношений с клиентами или вызвать санкции со стороны государства;
- угроза имуществу банка в форме его хищения или умышленного повреждения, а также сознательного провоцирования к осуществлению или непосредственного осуществления заведомо убыточных финансовых операций;
- угроза персоналу банка, реализация которой способна ухудшить состояние кадрового направления деятельности, например, в форме потери ценного специалиста или возникновения трудовых конфликтов.

б) По признаку источника угрозы (субъекта агрессии) выделяются:

- угрозы со стороны конкурентов, т.е. отечественных и зарубежных банков, стремящихся к усилению собственных позиций на соответствующем рынке путем использования методов недобросовестной конкуренции, например, экономического шпионажа, переманивания высококвалифицированных сотрудников, дискредитации соперника в глазах партнеров и государства;
- угрозы со стороны нелояльных сотрудников банка, осознанно наносящих ущерб его безопасности ради достижения личных целей, например, улучшения материального положения, карьерного роста, мщения работодателю за реальные или мнимые обиды и т.п.

в) По экономическому характеру угрозы выделяются:

- угрозы имущественного характера, наносящие банку прямой финансовый ущерб, например, похищенные денежные средства и товарно-материальные ценности, сорванный контракт, примененные штрафные санкции;
- угрозы неимущественного характера, точный размер ущерба от реализации которых обычно невозможно точно определить, например, сокращение обслуживаемого рынка, ухудшение имиджа банка в глазах его клиентов и деловых партнеров, утеря ценного специалиста.

г) По вероятности практической реализации угрозы выделяются:

- потенциальные угрозы, практическая реализация которых на конкретный момент имеет лишь вероятностный характер (соответственно, у субъекта управления есть время на их профилактику или подготовку к отражению);
- реализуемые угрозы, негативное воздействие которых на деятельность субъекта управления находится в конкретный момент в различных стадиях развития (соответственно, у субъекта имеются шансы на их оперативное отражение в целях недопущения или минимизации конечного ущерба);

- реализованные угрозы, негативное воздействие которых уже закончилось и ущерб фактически нанесен.

Таким образом, угроза — это начавший реализовываться по нежелательному варианту риск либо заранее известный сценарий неблагоприятного развития событий, соответственно выходящий за рамки понятия нормальной неопределенности условий бизнес деятельности.

Как известно, любая фирма в процессе своей деятельности подвергается разного рода рискам, наиболее неприятным результатом действия, которых является потеря вложенных средств. Организация рискует как собственными, так и привлеченными средствами. Однако потери в случае их возникновения относятся в первую очередь на собственный капитал, и только когда собственных средств недостаточно, потери начинают нести кредиторы. Таким образом, капитал играет роль защитного механизма для обеспечения сохранности средств кредиторов. Однако рост доли капитала в общей сумме средств предприятия в большинстве случаев означает сокращение прибыли, в чем собственники предприятия совсем не заинтересованы.

Система ограничения банковского риска является ключевым моментом, призванным обеспечить устойчивость и безопасность финансово-кредитной организации. Основное место в этой системе принадлежит показателю достаточности капитала. В мировой практике анализу величины собственного капитала банка отводится особая роль.

Соотношение собственного капитала и величины активов показывает, какая часть последних может быть потеряна без нанесения ущерба интересам кредиторов. Естественно, чем больше указанное соотношение, тем меньшему риску подвергаются кредиторы при прочих равных условиях. Не являются исключением в этом отношении и банки, но как финансово-кредитным

организациям им присуща одна особенность: во вкладываемых средствах подавляющая доля приходится на заемные и привлеченные.

Банк, выступая в качестве посредника, действующего от своего имени, но за счет клиента, трансформирует финансовые ресурсы в пространстве и во времени. Банк при этом является одновременно заемщиком и кредитором. Его основной доход - разница между уплаченными процентами по привлеченным средствам и полученными процентными выплатами. Размер банковской маржи не может быть большим, так как в противном случае привлечение средств банков для предприятий станет невыгодным и будет осуществляться непосредственно через фондовый рынок. Таким образом, для обеспечения выплаты банком своим акционерам доходов не ниже среднерыночных объем привлеченных средств многократно превышает собственный капитал, но при этом должна быть обеспечена и сохранность средств кредиторов.

На протяжении многих лет в разных странах в качестве механизма, обеспечивающего сохранность средств клиентов банка, использовалось соотношение между размером собственного капитала и активов. Этот показатель иногда имел модификации в виде отношения собственного капитала и пассивов, собственного капитала и привлеченных, заемных средств. Анализ данных коэффициентов с помощью балансового уравнения показывает их качественную тождественность. Однако все они не учитывали особенностей специализации банков, которая влияла на степень рискованности вложений. Например, активы банка, осуществляющего вложения преимущественно в акции, имеют более высокую степень риска, чем у ипотечного банка. В результате возможна ситуация, когда при равном соотношении между капиталом и активами одни банки способны полностью покрыть возникающие потери, а другие нет. Общепринятым способом борьбы с данным недостатком стало определение нормативов соотношения собствен-

ных средств с активами для различных групп банков в зависимости от специализации.

Взвешивание активов с учетом риска позволяет довольно точно определить относительный размер риска, присущего банку. В этом случае капитал сопоставляется с величиной риска данного банка, характеризующей не только масштаб его деятельности (размер активов), но и степень рискованности вложений.

Для оценки состояния активов коммерческого банка их подразделяют на группы в зависимости от степени риска вложений и возможной потери части стоимости. Степень банковского риска учитывает высокий, средний и низкий риски в зависимости от расположения по шкале рисков. Степень банковского риска характеризуется вероятностью события, ведущего к потере банком средств от данной операции, и выражается в процентах. Активы коммерческого банка делятся на 5 групп, при этом отдельным категориям и группам активов присваиваются соответствующие поправочные коэффициенты (или проценты), отражающие степень риска их потери.

В группу 1 входят активы, свободные от риска; в группы 2 и 3 - активы с минимальным риском; в группу 4 включены активы с повышенным риском; группу 5 составляют активы с максимальным риском.

Несмотря на проведенную выше группировку активов один и тот же риск может иметь различную степень. Это зависит от возможностей его гарантирования, страхования и других методов регулирования. Например, долгосрочные ссуды банка, выданные на строительство нового предприятия, имеют риск 100%. При страховании этой ссуды степень риска уменьшается до 50% (при условии страхования в объеме 50-90% ссуды). Таким образом, особенности определения степени банковского риска связаны с субъективным подходом к активам банка. В каждом отдельном случае

необходимо самостоятельное определение банками вероятности потери средств в результате той или иной операции.

На основании группировки активов по степени риска делают корректировку балансовой суммы активов. Активы, взвешенные с учетом риска, определяются следующим образом:

$$А_р = А_о \times К_р,$$

где $А_р$ - активы, взвешенные с учетом риска их потерь; $А_о$ - активы по отдельным операциям; $К_р$ - коэффициент риска.

Группировка активов банка ОАО Банк ВТБ (Азербайджан) по степени риска их вложений и возможной потери части стоимости используется для исчисления показателей достаточности капитала банка (таб.2.2.).

Анализ деления капитала банка на основной (или капитал 1-го уровня) и дополнительный (или капитал 2-го уровня) показывает, что у данного банка основную долю составляет капитал 1-го уровня, что положительно характеризует его качественную структуру, поскольку под основным капиталом понимается постоянная (неизменяемая по стоимости) часть капитала, которая может быть использована на покрытие любых убытков. Дополнительный (вторичный, капитал 2-го уровня)- величина, изменяемая в зависимости от изменения стоимости активов банка или рыночных рисков.

Таблица 2.2.

Структура капитала ОАО Банк ВТБ (Азербайджан)

Как видим из таблицы совокупный капитал (Məcmu kapital) складывается путем суммирования основного капитала за вычетом задолженностей (Tutulmalardan sonra I dərəcəli kapital) и капитала второго уровня (II dərəcəli kapitalın cəmi). С первой декады 2012 года по третью декаду 2014 года происходит увеличение совокупного капитала с 14,98105 тыс.манат до 47,97162 тыс. манат, то на 32,99057 тыс. манат. В заданный промежуток времени произошло одновременное увеличение активов банка, взвешенных с учетом риска, то есть если в конце 2012 года они составляли 85,98596 тыс.ман, в 2013 году - 211279,16 тыс.ман, то в конце 2014 года активы банка, взвешенные с учетом риска составляли - 261160,38 тыс.манат.

Норматив достаточности капитала банка регулирует (ограничивает) риск несостоятельности банка и определяет требования по минимальной величине собственных средств (капитала) банка, необходимых для покрытия кредитного, операционного и рыночного рисков. Это один из наиболее важных показателей надежности и безопасности банка. Характеризует способность банка нивелировать возможные финансовые потери за свой счет, не в ущерб своим клиентам.

В организационной структуре управления банком служба безопасности выступает в качестве одного из штабных, т.е. наделенных распорядительными полномочиями, подразделений. Она несет основную ответственность за эффективную защиту имущественных и неимущественных интересов кредитно-финансовой организации от рассматриваемого в настоящем курсе перечня угроз, получая для этого необходимые ресурсы и полномочия (рисунок 2.1.).

Рисунок 2.1.

Организационная структура управления ОАО Банк ВТБ (Азербайджан)

Особое место рассматриваемой здесь службы среди других структурных подразделений банка определено самим характером ее деятельности. Она включает в себя исполнение сотрудниками службы безопасности по отношению к другим работникам фирмы многочисленных контрольных, ограничивающих и пресекающих функций. Это вызывает подсознательную негативную реакцию даже у той части персонала, которая в силу своего должностного уровня не может не понимать вынужденную необходимость подобных действий. Ощущая такое отношение, сотрудники службы безопасности часто «идут на принцип», т.е. намеренно демонстрируют свои полномочия, ведут себя откровенно агрессивно – недружелюбно по отношению к работникам других подразделений банка и, тем самым, лишь усугубляют ситуацию. Поэтому отношения между службой безопасности и остальной частью трудового коллектива банка всегда имеют потенциально конфликтный характер. Это определяет необходимость регулярных профилактических мероприятий, направленных, с одной стороны, на основную часть персонала, а с другой – на сотрудников самой службы безопасности. В противном случае становится невозможным обеспечить практическую реализацию одного из базовых методических требований к организации управления безопасностью, а именно вовлечения в этот процесс всех сотрудников и инстанций.

Выбор принципиального подхода к организации службы безопасности в конкретном банке определяется многими факторами.

Главным из них является избранная ее руководством стратегия по рассматриваемому направлению деятельности, а именно – степень ее активности. Чем более активна эта стратегия, тем большие требования предъявляются к службе безопасности, соответственно, сложнее ее внутренняя структура, больше численность персонала. Например, при ориентации руководства кредитной организации на проведение стратегии пассивной защиты от возможных угроз, явно нецелесообразно создание в составе службы спе-

циального аналитического подразделения, занимающегося экономической разведкой.

Вторым фактором является ориентация руководства на возможное использование услуг специализированных структур в лице частных охранных агентств. Ниже проводится сравнительный анализ трех возможных подходов.

Первый из них предполагает полный отказ от их услуг и характерен, обычно, для крупных банков, ориентированных на проведение стратегии «упреждающего противодействия». В этом случае кредитная организация вынуждена формировать собственную службу безопасности «по полной программе», комплектуя ее всеми необходимыми специалистами и обеспечивая соответствующими ресурсами.

Основным преимуществом данного варианта является большая степень доверия со стороны руководства банка к собственным сотрудникам, входящим в постоянный штат организации. При правильной организации управления деятельностью службы и, прежде всего, ее персоналом, появляется возможность воспитания у него «корпоративного духа». Недостатками данного варианта выступают высокий уровень затрат на содержание подобной службы, а для периферийных банков – объективные сложности с комплектацией ее высококвалифицированными сотрудниками всех необходимых специальностей. Принципиальная организационная структура управления службы безопасности, созданной по такому варианту, представлена на рисунке 2.2.

Второй, прямо противоположенный, подход предполагает минимизацию штатных сотрудников службы безопасности банка, с возложением основных ее функций на сторонние специализированные структуры, привлекаемые на контрактной основе.

Привлекательность данного подхода обеспечивается многими факторами, среди которых можно выделить:

- меньшую капиталоемкость;

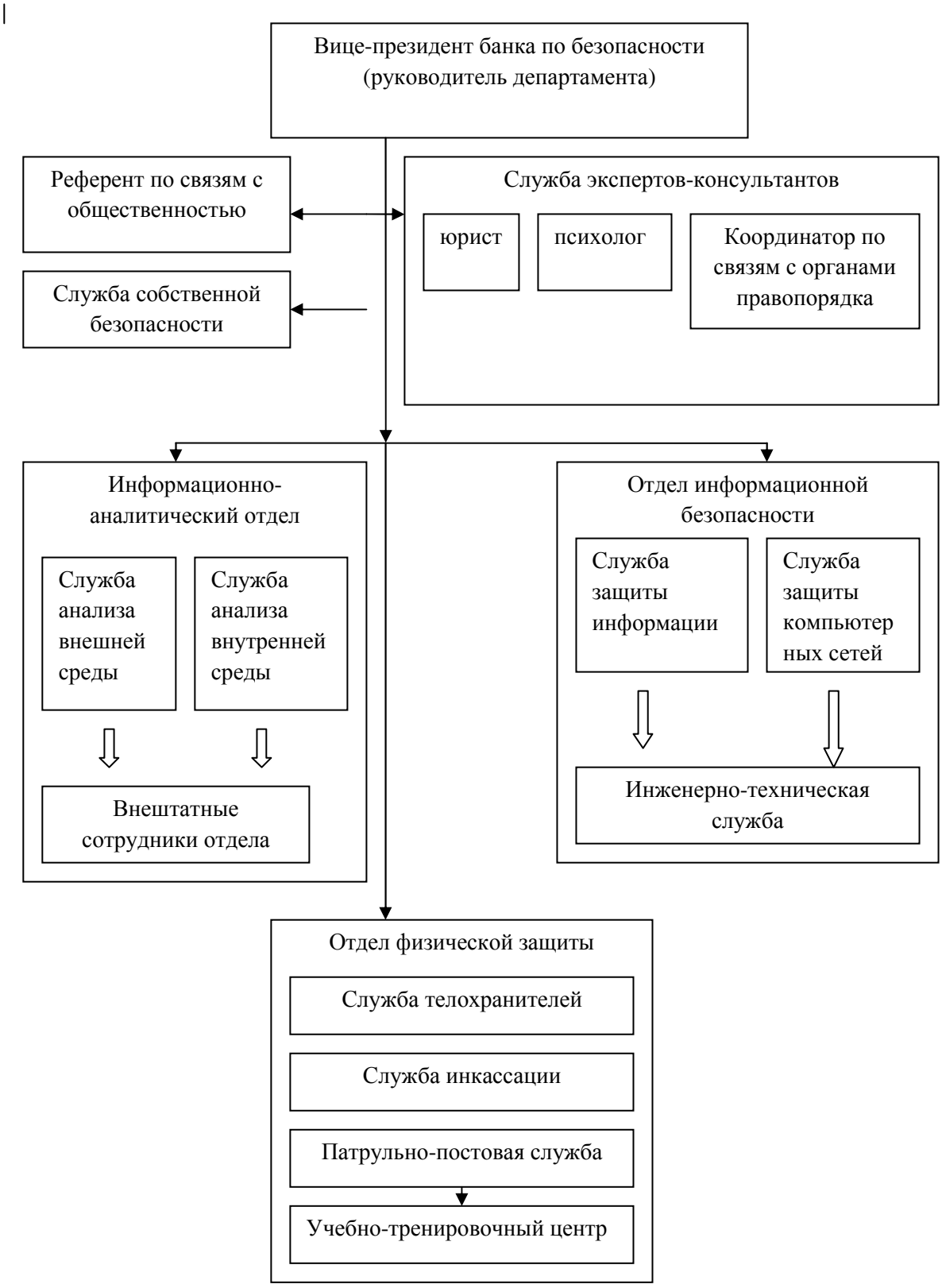


Рисунок 2.2.

Типовая структура департамента безопасности банка

- гарантированный контрактом профессионализм привлеченных из специализированных структур сотрудников;
- в отечественных условиях – отсутствие многих ограничений, связанных с частной охранной деятельностью.

Однако, в отличие от предприятий в других отраслях экономики, российские и зарубежные банки используют данный подход крайне редко.

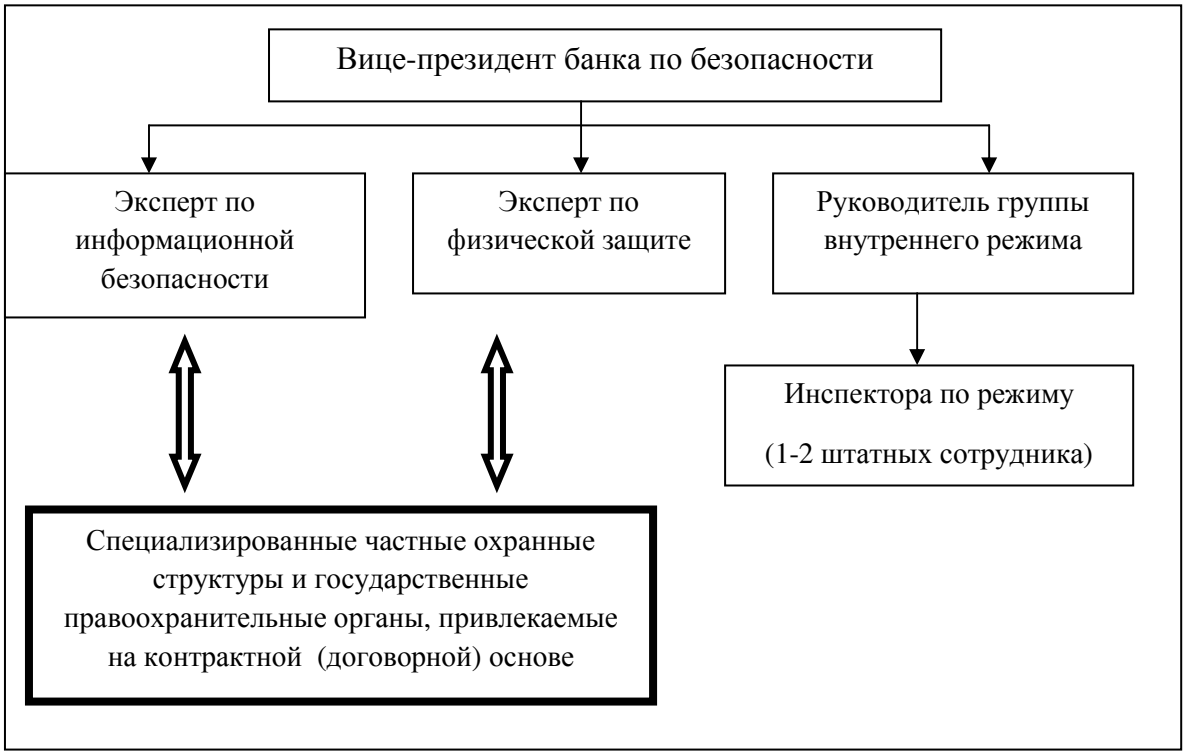
Это определяется в первую очередь низким доверием к любым сторонним для конкретного банка структурам.

Рекомендации по применению: для государственных и небольших банков, реализующих пассивную конкурентную стратегию.

Принципиальная организационная структура управления службы безопасности, созданной по такому варианту, представлена рисунке 2.3.

Рисунок 2.3.

Типовая структура службы безопасности банка



Третий, компромиссный, подход предполагает возможность частичного использования услуг специализированных частных структур для

выполнения локальных задач. Он ориентирован на кредитные организации, реализующие стратегию «адекватного ответа» и при этом относительно редко сталкивающиеся со сложными задачами обеспечения собственной безопасности, например, утечкой конфиденциальной информации, хищением денежных средств с использованием компьютерных технологий, шантажом и угрозами в адрес сотрудников. В соответствии с изложенными выше требованиями к организации системы, для таких банков целесообразно ориентироваться на принцип «разумной достаточности» и не включать в постоянный штат службы безопасности сотрудников, чей опыт и квалификация будет востребована от случая к случаю [15].

2.2. Методы противодействия угрозам имущественной безопасности банка

Организация контроля над соблюдением персоналом правил обеспечения безопасности и его лояльностью, контроль по рассматриваемому направлению осуществляется службой безопасности банка. В зависимости от ее организационной структуры, им могут заниматься либо уполномоченные сотрудники специализированных подразделений (отдела информационной безопасности, физической защиты и т.п.), либо инспектора специального подразделения контроля внутреннего режима. Основными задачами проведения данной работы выступают:

- оценка общей эффективности управления обеспечением безопасности в конкретных структурных подразделениях банка;
- контроль над лояльностью конкретных сотрудников;
- выявление конкретных нарушений и их виновников.

Исходя из этого, организация данной работы осуществляется службой безопасности одновременно по нескольким направлениям.

Профилактический контроль над соблюдением правил обеспечения безопасности в трудовых коллективах банка проводится с использованием различных методов и процедур, в частности:

- плановых и внезапных проверок, в процессе которых служба безопасности проверяет соблюдения в структурных подразделениях правил работы с конфиденциальной информацией, хранения денежных и иных ценностей, а также работоспособность технических средств защиты;
- мониторинга ситуации с использованием специальных технических средств наблюдения (например, видеокамер, первоначально установленных в качестве технических средств защиты имущества и персонала);
- мониторинга ситуации силами нештатных информаторов службы безопасности из числа сотрудников соответствующих подразделений банка.

По результатам оперативного контроля служба безопасности готовит специальные отчеты для президента банка, информационные записки на имя руководителей его структурных подразделений. При необходимости она организует проведение специальных совещаний у руководства, собраний в трудовых коллективах подразделений, готовит проекты приказов о поощрениях или взысканиях.

Контроль личной лояльности персонала осуществляется службой безопасности в отношении сотрудников:

- занимающих ключевые рабочие места (кроме должности президента), обеспечивающие доступ к особо конфиденциальной информации или возможность принимать решения стратегического характера;
- привлекших внимание службы безопасности своим поведением или иными фактами, ставящими под сомнение их лояльность.

В зависимости от цели и используемых методов контроля могут быть выявлены прямые нарушения в деятельности сотрудника, являющиеся основанием для передачи соответствующего иска в судебные или заявления в правоохранительные органы, увольнения, иных форм дисциплинарных

взысканий. К числу подобных нарушений относятся подтвержденные соответствующими документами или иными материалами факты:

- проникновения в закрытые компьютерные базы данных и операционные системы с целью их копирования или проведения несанкционированных операций по счетам;
- любых попыток хищения денежных средств или материальных ценностей;
- коррупции в форме получения взяток от клиентов или партнеров банка;
- успешной вербовки сотрудника субъектами потенциальных угроз;
- склонения подчиненных к нарушению доверия работодателя;
- нарушений правил внутренней безопасности банка, в том числе и не приведших к реализации соответствующих угроз.

Кроме того, по результатам персонифицированного контроля служба безопасности может выявить факторы, определяющие сомнения в потенциальной лояльности сотрудника, например:

- необъяснимое объективными причинами внезапное улучшение материального положения сотрудника или контактирующих с ним родственников;
- не вызванные служебной необходимостью контакты с представителями субъектов потенциальных угроз;
- изменение образа жизни сотрудника или появление привычек и личностных качеств, делающих его уязвимым для вербовки и шантажа;
- зафиксированные регулярные высказывания недовольства работодателем, служебным положением, доходами и т.п.

В этом случае, в зависимости от занимаемого сотрудником служебного положения, профессиональных качеств, отзывов руководителя, к нему могут

быть применены разнообразные методы воздействия. По отношению к малоценным для банка работникам рекомендуется невозобновление трудового контракта после истечения его срока, а до этого момента постоянный контроль над их поведением. В остальных случаях с сотрудником должна быть проведена индивидуальная профилактическая работа силами непосредственного руководителя, психолога службы персонала или специалиста службы безопасности. Результаты персонифицированного контроля должны отражаться в системе специального учета самой службы безопасности и в индивидуальном досье сотрудника.

2.3. Основные элементы политики противодействия внутреннему мошенничеству

Оценка эффективности управления кадровой безопасностью является необходимым элементом рассматриваемой системы. Она позволяет решить несколько прикладных задач, например, осуществлять статистический анализ вероятности негативной реализации тех или иных угроз, а также объективно оценивать результативность деятельности службы безопасности. В отличие от большинства других направлений менеджмента здесь не всегда можно точно подсчитать обеспеченный экономический эффект. В частности, затруднительно определить возможные потери от своевременно пресеченных угроз. По некоторым видам угроз, например, в адрес сотрудников кредитной организации, прямой эффект невозможно рассчитать в принципе. Поэтому приходится опираться на результаты не только прямой, но и косвенной оценки.

Приведем перечень критериев, для решения этой задачи:

1) динамика текучести кадров в форме инициативных увольнений сотрудников, в том числе ушедших на работу к непосредственным конкурентам;

2) общее количество выявленных угроз с дифференциацией на угрозы, пресеченные в полном объеме, пресеченные частично, негативно реализованные в полном объеме (в сравнении с предыдущими периодами);

3) прямой финансовый ущерб, нанесенный организации в результате частично и полностью реализованных угроз;

4) потенциальный ущерб, который могли бы нанести организации полностью или частично пресеченные угрозы;

5) результаты реализации плановых профилактических мероприятий;

6) отсутствие обоснованных претензий к службе безопасности со стороны правоохранительных органов, собственных подразделений и отдельных сотрудников.

Факторы, влияющие на внутреннее мошенничество:

1) Слабая система внутреннего контроля или ее отсутствие.

2) Отсутствие адекватного разделения полномочий.

3) Неадекватная компенсационная политика.

4) Отсутствие кодекса корпоративной этики и четких правил «что хорошо, а что плохо» внутри компании.

5) Пренебрежительное отношение со стороны руководства и персонала к этическим ценностям компании.

Организация системы внутреннего контроля Банка ВТБ (Азербайджан) через:

1) Наблюдение со стороны Наблюдательного Совета

2) Наблюдение со стороны Совета Директоров Банка

3) Функциональные обязанности и контроль исполнительного руководства всех уровней

4) Соблюдение функциональных обязанностей специалистов всех уровней

5) Организация работы служб внутреннего аудита и службы безопасности относительно проверки, оценки рисков и предупреждения, блокировки возможных рисковых операций.

ОАО Банк ВТБ (Азербайджан) руководствуется «Политикой по управлению рисками», которая устанавливает основные задачи, принципы и механизмы внутренних процессов формирования и функционирования системы управления рисками.

Общая структура системы органов/структурных подразделений, задействованных в управлении рисками в Банке, имеет следующие уровни:

- Верхний уровень – Общее Собрание Акционеров, Наблюдательный Совет и Аудиторский Комитет Банка;
- Средний уровень – Правление Банка (включая Председателя Правления Банка), Служба внутреннего аудита и комитеты Банка;
- Нижний уровень – структурные подразделения и отдельные сотрудники Банка.

Компетенцией Наблюдательного Совета Банка является:

- утверждение политик Банка, в том числе Кредитной политики;
- утверждение правил по управлению отдельными рисками;
- принятие решения о создании капитальных резервов Банка;
- разрешение на заключение сделок, сумма которых превышает 25 (двадцать пять) процентов стоимости чистых активов Банка;
- разрешение на заключение от имени Банка сделок, сумма которых превышает 50 (пятьдесят) процентов уставного капитала Банка;
- утверждение сделок с аффилированными лицами Банка и лицами, действующими от их имени, в случаях, предусмотренных законодательством Азербайджанской Республики;
- создание и ликвидация комитетов Банка (за исключением Аудиторского Комитета), утверждение их положений;

- определение лимитов по операциям Банка и делегирование этого полномочия Комитету по управлению рисками Банка;
- принятие решения о списании с баланса Банка безнадежных активов.

Компетенцией Аудиторского Комитета Банка является:

- определение аудиторской политики и стратегии Банка;
- утверждение внутренних аудиторских планов и осуществление контроля за деятельностью Службы внутреннего аудита Банка [34].

Сегодня наличие внутреннего аудита в организациях рассматривается как важный фактор эффективности вне зависимости от того, есть в организации система менеджмента качества (экологии и т.д.) или нет. Наличие системы внутреннего аудита повышает доверие инвесторов и других заинтересованных сторон, повышает их уверенность в рациональном использовании компанией ресурсов, сохранности активов, оптимизации компанией рисков деятельности, прозрачности компании, а также в соответствии организации деятельности компании лучшим практикам корпоративного управления. Компетенцией Службы внутреннего аудита Банка является непрерывный контроль над эффективностью деятельности систем внутреннего контроля и управления рисками.

Система противодействия мошенничеству основывается на оценке рисков мошенничества и должна включать в себя три линии обороны.

1 линия обороны — кодекс поведения сотрудников и политики, связанные с ним. Формирование соответствующей атмосферы, позиции нетерпимости к мошенничеству, культуры этики и высокой честности.

2 линия обороны — система внутреннего контроля.

3 линия обороны — деятельность служб внутреннего аудита и внутренней безопасности.

Профилактика мошенничества должна начинается с тщательного отбора кандидата, проверки его безупречной деловой репутации, сбора и проверки рекомендаций:

1) При оформлении в штат новый сотрудник обязательно должен знакомиться под роспись с внутренними инструкциями, политикой внутренней безопасности, политикой противодействия внутреннему мошенничеству, правилами внутреннего трудового распорядка, должностной инструкцией и другими нормативными документами, регламентирующими деятельность подразделения. Лист ознакомления хранится в личном деле сотрудника.

2) Для новых сотрудников должно быть обязательным адаптационное обучение. В программе тренинга не только информация о банке, его истории, достижениях, организационной структуре и культуре (миссия, ценности, традиции, культура этики и высокой честности), а также вопросы информационной безопасности и политики банка по противодействию мошенничеству.

3) Тестирование в банке должно быть нормой. Кроме профессиональных тестов, новые сотрудники за 2 недели до окончания испытательного срока должны сдать тест на знание кодекса поведения сотрудника, политики стандартов и политики противодействия мошенничеству.

4) Все сотрудники проходят специальное тематическое обучение по вопросам противодействия мошенничеству. Такое обучение, как правило, организовано совместными усилиями HR-департамента и департамента безопасности.

Таким образом, основным требованием к системе обеспечения собственной безопасности банка является комплексный подход к организации защиты от всех возможных угроз, исключающий наличие незащищенных или плохо защищенных объектов. При формировании перечня используемых методов защиты от возможных угроз безопасности банка однозначный приоритет должны иметь методы профилактического характера.

ГЛАВА III. Совершенствование механизмов обеспечения безопасности современного бизнеса

3.1. Правовое совершенствование информационного обеспечения безопасности бизнеса

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность бизнеса становится обязательной. Под угрозой безопасности информации в бизнесе понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

В соответствии с действующим в стране законодательством информационные правоотношения — это отношения, возникающие при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации [6,2]. Правовое регулирование в области информационных правоотношений осуществляется рядом нормативных актов:

- Законом Азербайджанской Республики "О Средствах массовой информации",
- Законом Азербайджанской Республики "Об авторском праве и смежных правах"
- Законом Азербайджанской Республики "Об информации, информатизации и защите информации".
- Законом Азербайджанской Республики « О Коммерческой тайне».

Важным шагом является признание информации в качестве объекта гражданских прав.

Анализ действующего законодательства показывает, что:

1.Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [6,2].

2.Правовой защите подлежит любая документированная информация**,** т. е. информация, облеченная в форму, позволяющую ее идентифицировать [6,3].

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, может быть конфиденциальной, а предназначенная для неограниченного круга лиц — массовой**.**

5. Ограничения (установление режима) использования информации определяются законом или собственником информации, которые объявляют о степени (уровне) ее конфиденциальности. Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как государственная тайна, тайна переписки, телефонных переговоров, почтовых телеграфных или иных сообщений; тайна усыновления, служебная тайна, коммерческая тайна, банковская тайна, личная тайна, семейная тайна, информация, являющаяся объектом авторских и смежных прав, информация, непосредственно затрагивающая права и свободы гражданина или персональные данные и др.

6.Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является

нарушением его прав, т.е. неправомерной.

7. Неправомерное использование документированной информации наказуемо.

К уголовно наказуемым отнесены неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Таким образом, мы видим, что информационные отношения получили уголовно-правовую защиту. Из этого следует, что информация и информационные отношения стали новым объектом преступления**.** Известно, что большинство технологических инструментов обработки информации основывается на разнородных технических средствах, относящихся к различным классам и имеющих разнообразную физическую природу.

Компьютер является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением конфиденциальной документированной информации.

Согласно Статье 271 Уголовному Кодексу Азербайджанской Республики компьютерная информация- эта информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе электронно-вычислительных машин, или их сети.

В последнее время границы применения компьютеров заметно расширились. С каждым днем во всем мире увеличивается число пользователей всемирной компьютерной сети Интернет.

В то же время порожденные научно–техническим прогрессом различного рода проявления, правонарушения стимулировали возникновение

неизвестных ранее способов посягательства на охраняемые законом бизнес отношения. Одной из наиболее распространенных является, например, необходимость обеспечения надежной защиты от несанкционированного доступа к бизнес информации, коммерческой тайне компании. Вполне естественно, что руководители компаний принимают определенные меры безопасности. Юридическая охрана сферы применения компьютеров стала необходимой, а выполнение этой роли было возложено на уголовное право.

Согласно УК АР различают следующие виды преступлений в сфере компьютерной информации:

1. неправомерный доступ к компьютерной информации;
2. создание, использование и распространение вредоносных программ для ЭВМ;
3. нарушение правил эксплуатации электронно-вычислительных машин (ЭВМ), системы ЭВМ или их сети.

В частности, нормы о преступлениях в обозначенной сфере зафиксированы в трех статьях УК АР: ст. 272 (Неправомерный доступ к компьютерной информации), ст. 273 (Создание, использование и распространение вредоносных программ для ЭВМ) и ст. 274 (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети). Общий объект данной категории преступлений - общественные отношения в сфере обеспечения информационной безопасности, а к непосредственным объектам преступного посягательства относятся базы и банки данных конкретных компьютерных систем или сетей, их отдельные файлы, а также компьютерные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации [9].

Согласно ст. 272 Уголовного Кодекса Азербайджанской Республики, уголовная ответственность за неправомерный доступ к компьютерной

информации наступает, если это деяние повлекло за собой, хотя бы одно из следующих негативных последствий:

а) уничтожение, блокирование, модификацию либо копирование информации;

б) нарушение работы ЭВМ или их сети.

Огромный вред наносят нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это может не только привести к сбоям в работе оборудования, но в некоторых случаях и полностью парализовать работу предприятия, учреждения или организации. Поэтому законодательно установлено, что в случае причинения существенного вреда в результате указанных действий, а также при наступлении по неосторожности тяжких последствий описанные деяния наказуемы в уголовном порядке, если они повлекли уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ (ст. 274 УК АР).

С субъективной стороны преступление может быть совершено по неосторожности в виде как небрежности, так и легкомыслия. Субъект преступления специальный - лицо, имеющее доступ к эксплуатации упомянутых технических средств. Это могут быть программисты, операторы ЭВМ, другие лица, по работе имеющие к ним доступ.

В настоящее время можно выделить свыше 20 основных способов совершения компьютерных преступлений и около 40 их разновидностей. И их число постоянно растет.

Основной объем прав на производство информации, относимой к коммерческой тайне, содержится в Законе Азербайджанской Республики «О коммерческой тайне». Под коммерческой тайной, согласно закону, понимаются сведения, связанные с производственной, технологической, управленческой, финансовой и другой деятельностью юридических и

физических лиц, разглашение которых без согласия владельца может причинить ущерб их законным интересам. Помимо этого статья 2 закона дает следующие понятия:

1) «ноу-хау» - сведения, отнесенные как результат умственной деятельности к коммерческой тайне, не охраняемые патентом согласно законодательству или по соображениям владельца;

2) Владелец коммерческой тайны – юридическое или физическое лицо, владеющее на законных основаниях коммерческой тайной;

3) Конфидент коммерческой тайны – юридическое или физическое лицо, получившее на законных основаниях коммерческую тайну у владельца коммерческой тайны;

4) Носители коммерческой тайны- материальные и нематериальные объекты, выражающие коммерческую тайну в виде знаков, изображений, формул, технологических процессов, сигналов и в другой форме;

5) Режим коммерческой тайны – установленная владельцем коммерческой тайны или конфидентом система правовых, организационных, технических и других мер по ограничению овладения коммерческой тайной;

6) Распространение коммерческой тайны- разглашение коммерческой тайны другим лицам путем нарушения соответствующего законодательства или договорных условий;

7) Незаконные способы овладения коммерческой тайной-обретение коммерческой тайны такими незаконными способами, как хищение, фотографирование документов, снятие с них копий, применений силы или угроза, дача взятки, нарушение или подстрекательство (принуждение) к нарушению обязательств по соблюдению режима коммерческой тайны, подключение к каналам передачи информации, подслушивание переговоров и ведение наблюдений [4].

Согласно трудовому договору или соглашению о соблюдении режима коммерческой тайны конфиденты коммерческой тайны обязаны после прекращения трудового договора соблюдать режим коммерческой тайны до отмены отнесенности информации к коммерческой тайне.

Лица, получающие незаконным путем или распространяюшие информацию, представляющую коммерческую тайну, несут ответственность в порядке, предусмотренном соответствующим законодательством Азербайджанской Республики.

Процесс комплексной защиты информации должен осуществляться непрерывно на всех этапах бизнес деятельности. Реализация непрерывного процесса защиты информации возможна только на основе систем концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации. В то же время как невозможно в полной мере выделить информационную составляющую в деятельности предприятия, так очень сложно разграничить правовое регулирование этой сферы различными отраслями права.

Совершенствование нормативно-правовой базы в области обеспечения информационной безопасности бизнеса должен включать:

1. Государственную политику информационной открытости как условие предупреждения экономических преступлений. Перевод документальных массивов информации в электронные и введение их в гражданский оборот в открытом доступе.
2. Совершенствование механизма гражданско-правовой ответственности предпринимателей по договорам.

3. Гарантии равного права доступа субъектов предпринимательской деятельности к информационным ресурсам.
4. Правовая защита интересов субъектов предпринимательской деятельности на внешнем рынке.
5. Государственные меры по защите интеллектуальной собственности.
6. Государственная поддержка практики эффективного использования объектов интеллектуальной собственности в деловом обороте.
7. Государственная защита объектов национальной интеллектуальной собственности на международном рынке.
8. Государственная поддержка программ укрепления деловой репутации авторитетных отечественных компаний, в том числе выходящих на зарубежные рынки.
9. Создание благоприятного информационного поля для развития азербайджанского бизнеса за рубежом.
10. Интеграция национальных средств массовой информации с международными сетями распространения экономической информации.
11. Совершенствование патентного дела в Азербайджане.

3.2. Внедрение эффективной структуры службы безопасности фирмы

Одним из инструментов по обеспечению защиты безопасности фирмы является создание на его базе собственной эффективной службы безопасности. Не случайно уважающие себя и умеющие считать деньги западные бизнесмены тратят на содержание собственной системы безопасности до 25% дохода [20,70].

В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы самой компании с развитой

штатной численностью.

Если предприятие создает свои собственные штатные подразделения охраны, то они организационно могут быть объединены в службу охраны. Служба охраны включает посты охраны, группы (подразделения) сотрудников охраны (в том числе подразделение личной охраны руководства и персонала), группу охраны и сопровождения материальных ценностей и грузов, «тревожную» группу (группу быстрого реагирования), а также подразделения сторожевых собак (при необходимости). Однако наиболее часто подразделения охраны наряду с другими подразделениями, решающими задачи по различным направлениям защиты информации, объединяются в службу безопасности предприятия. Если предприятие создает свою собственную службу безопасности, то она как правила становиться самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности, как правило, заместителя руководителя предприятия по безопасности.

В крупных службах безопасности возможно введение должностей помощников (референтов) начальника.

Организационно служба безопасности должна состоять из следующих структурных единиц:

- отдел режима и охраны, в составе сектора режима и сектора охраны;
- отдел защиты информации;
- инженерно-техническая группа;
- группа безопасности внешней деятельности.

Приведенная структура службы безопасности не универсальна и должна корректироваться под определенную организацию. В частности, в нее могут быть введены новые отделы, например отдел пожарной безопасности, группа управления персоналом или группа сопровождения грузов. Как правило, формирование или реформирование структуры

собственной безопасности осуществляется по мере понимания задач, которые должны ею решаться на текущий момент.

К основным функции деятельности службы безопасности можно отнести:

1. Установление обстоятельств недобросовестной конкуренции со стороны других предприятий.

2. Сбор сведений по уголовным делам. Уголовные дела, к расследованию которых подключается служба безопасности, условно можно разделить на две группы: возбужденные в связи с совершением преступлений против персонала предприятия и преступления против собственности учредителя. Например, кража личного имущества у сотрудника фирмы сама по себе не обязывает сотрудников службы безопасности подключаться к расследованию этого преступления, однако, в том случае, если среди этого имущества окажутся документы предприятия-учредителя, то ситуация меняется противоположным образом. К наиболее распространенным преступлениям второй группы относятся кражи, грабежи, мелкие хищения, поджоги и т.д. Весьма актуальными для сотрудников службы безопасности стали преступления в сфере экономической деятельности и против интересов службы в коммерческих организациях.

3. Расследование фактов разглашения коммерческой тайны предприятия.

4. Сбор информации о лицах, заключивших с предприятием контракты. Предприятие обычно заключает два типа контрактов: коммерческий (документ, представляющий собой договор поставки товаров или предоставления услуг) и трудовой (вид трудового договора, заключающегося в письменной форме со своими постоянными или временными работниками).

5. Поиск утраченного имущества предприятия Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия.

6. Расследование фактов неправомерного использования товарных

(фирменных) знаков предприятия.

8. Розыск без вести пропавших сотрудников. Сотрудники службы безопасности подключаются к розыску без вести пропавшего сотрудника только в том случае, если есть основания предполагать, что его отсутствие на работе приведет (может привести) к реальному или потенциальному ущербу предприятию.

9. Выявление некредитоспособных партнеров. Служба безопасности обязана выявлять некредитоспособных партнеров, как до заключения, так и в процессе реализации договора и своевременно информировать об этом руководство предприятия.

10. Выявление ненадежных деловых партнеров. Ненадежность делового партнера может определяться большим количеством сорванных по его вине сделок с другими фирмами; несвоевременным и некачественным выполнением условий заключенных договоров; значительным количеством в фирме ранее судимых лиц; неуважительным отношением к авторскому или патентному праву и. т.д. Способность службы безопасности своевременно выявить хотя бы отдельные параметры ненадежности будущих или настоящих деловых партнеров в значительной степени может повлиять на степень экономической безопасности предприятия-учредителя.

11. Сбор сведений по гражданским делам. Сбор сведений по гражданским делам служба безопасности осуществляет во взаимодействии с представителем предприятия-учредителя на суде как до, так и во время рассмотрения их на судебных заседаниях.

12. Сбор информации для проведения деловых переговоров. Сотрудники службы безопасности участвуют в сборе информации как на стадии подготовки к переговорам, так и во время их проведения. Например, в процессе подготовки к переговорам сведения об участниках будущих переговоров, их сильных и слабых сторонах, их позициях и планах ведения переговоров, подготовленных материалах, конкурентоспособности и платежеспо-

собности делового партнера и т.д. Во время проведения переговоров служба безопасности должна поставлять информацию об изменениях позиции партнеров по переговорам, о возможных попытках с их стороны шантажировать, подкупать членов делегации предприятия-учредителя, проведения разведывательных мероприятий в отношении их и т.д.

13. Защита жизни и здоровья персонала от противоправных посягательств.

14. Охрана имущества предприятия.

15. Обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий. В зависимости от их типа мероприятий меняется и содержание деятельности службы безопасности. Например, при проведении закрытых совещаний основное внимание уделяется, прежде всего, защите сведений, составляющих коммерческую тайну, на выставках необходимо принимать меры к недопущению кражи или порчи имущества предприятия; при проведении концертов основное внимание уделяется физической безопасности людей и т. д.

16. Консультирование и представление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности. В обязанности службы безопасности входит не только консультирование и дача рекомендаций сотрудникам предприятия по вопросам обеспечения безопасности, но и ее реализация.

17. Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Эффективность, а значит, успех деятельности любой службы безопасности находится в прямой зависимости от:

- соответствия квалификации сотрудников охраны и их морально-нравственных качеств решаемым задачам;

- умения продавать способность людей выполнять свои функциональные обязанности в режиме «устойчивого равновесия».

Организация кадрового обеспечения охранного предприятия, в связи с изложенным, приобретает для его руководства особую важность, особенно при определении путей оптимизации управления его структурами в интересах повышения эффективности и качества деятельности охраны. К приоритетам кадровой работы службы безопасности относятся следующие моменты:

Во-первых, концептуальный подход. Практика показывает, что успешное управление охранным предприятием возможно лишь при соблюдении следующих непреложных правил кадровой работы. Прежде всего к таким правилам следует отнести наличие утвержденной руководством формализованной программы и концепции кадрового обеспечения безопасности объекта. Второй составляющей является строгое соблюдение принципов подбора и процесса найма сотрудников, к которым относятся изучение кандидатов, современные методы проверки их благонадежности, психологические характеристики, оценка возможностей кандидатов, уровня их опыта и способностей в специфических областях деятельности службы безопасности и т. п.

Во-вторых, принципы организации кадровой работы. Служба безопасности в этой деятельности должна придерживаться следующих принципов: 1) кадровая работа не для тех, кто преследует «особые интересы»; 2) гарантией надежности кадровика и качества его работы являются честность и достоинство, опыт и квалификация; 3) кадровая работа должна быть сориентирована на цели и задачи, намеченные руководством службы безопасности; 4) по своему составу подразделения службы безопасности должны представлять собой постоянные группы единомышленников, заинтересованных в повседневной совместной работе, успех которой зависит от их «оперативной репутации»; 5) эффективная кадровая работа предполагает

постоянный контакт с представителями других субъектов «единого кадрового поля», при этом отношения такого рода должны базироваться прежде всего на потребностях обеспечения защиты конкретных объектов [24].

В-третьих, кадровый потенциал. Изучение и оценка способностей кандидата к будущей профессиональной деятельности — один из важнейших элементов системы отбора кадров. При определении критериев отбора кандидатов из числа лиц, приходящих с улицы, в интересах обеспечения собственной безопасности перед теми, кто в службе безопасности осуществляет профессиональный отбор, должны ставиться следующие задачи:

- выявление в среде кандидатов лиц, ранее имевших судимости, обладающих преступными связями и криминальными наклонностями;
- определение характера преступных склонностей, предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;
- установление фактов, свидетельствующих о морально-психологической ненадежности кандидата на работу, его неустойчивости, ущербности, уязвимости, алкогольной зависимости и т. п.;
- фиксирование психофизической готовности кандидата исполнять охранные функции, включая изучение его устойчивости к монотонным нагрузкам, предела утомляемости, готовности к вооруженному противодействию, уравновешенности характера;
- определение лояльности соискателя по отношению к руководству службы безопасности и его устойчивость к различным видам вербовочных подходов.

Служба безопасности при комплектовании своего кадрового состава должна использовать специально разработанную автоматизированную систему компьютерных тестов, включающих в себя несколько сот вопросов.

Основной акцент при этом делается на интеллект, психику, эмоционально-волевую сферу, честность и порядочность. Следует сказать, что эта практика дает 70% вероятного успеха по указанным выше критериям.

В-четвертых, профессиональный уровень и специальная подготовка. Естественно, что основное внимание при подборе сотрудников службы безопасности уделяется их уровню профессиональной подготовки (данные, характеризующие кадровый состав и его образовательный ценз: высшее образование, специальное образование и т. д.; количество сотрудников, работающих по найму и по контракту; и т. п.). Именно эти сведения позволяют определить уровень наличия у сотрудников базового опыта в области обеспечения безопасности и общей подготовки в специфических областях различных функциональных участков службы безопасности, а также судить о перспективах продолжения их карьеры в службе безопасности, необходимости повышения квалификации отдельных руководителей. Кроме того, такая информация дает возможность определить, на каких участках находятся наиболее опытные руководители.

К категории среднего руководящего состава службы безопасности предъявляются другие требования. Здесь важно знать о способности руководителя не только разработать программу защиты объекта, которая будет адекватной угрозам его безопасности, но и организовать противодействие им на современном уровне. Очень важно также, чтобы руководитель обладал способностью реально оценивать эффективность действующих систем охраны.

Универсальных рецептов, позволяющих полностью обезопасить фирму от негативных действий собственных сотрудников, пока еще нет, как нет и средств обеспечения стопроцентной безопасности. Однако есть возможность максимально снизить эту опасность, держать ее под контролем и избежать нежелательных последствий. Это — осознанная, организованная, последова-

тельная и целенаправленная кадровая политика. Она составляет столь же необходимое условие нормальной работы предприятия, как и продуманные бизнес-планы. Эта политика базируется на трех основных принципах: разумный отбор персонала с помощью современных методов; продуманная и грамотно построенная система вознаграждения и служебного роста; организационная культура, поддерживающая в фирме климат взаимоотношений, благоприятный для совместной работы персонала.

3.3. Совершенствование технических средств обеспечения безопасности бизнеса

В предыдущих параграфах магистрской работы мы рассмотрели физическую, экономическую, внутреннюю и информационную составляющие безопасности бизнеса. Наряду с технической составляющей они довольно тесно взаимосвязаны. Техническая безопасность считается пассивной, так как она не оказывает непосредственного воздействия на злоумышленника, в отличие от физической. Под технической системой безопасности понимается система раннего обнаружения угроз предприятию от стихийных бедствий, несанкционированного проникновения нарушителей и ошибочных либо неправомерных действий персонала или клиентов предприятия с использованием технических средств обнаружения угроз. При этом обнаружение, а зачастую нейтрализация и даже ликвидация угроз осуществляются с помощью различных технических средств и методов. Технические средства обеспечения безопасности выполняют функцию блокирования угроз, автоматического контроля целостности границ зон защиты объекта, обеспечивают возможность дистанционного визуального контроля, оперативного изменения степени защищенности охраняемого объекта (например, блокировка в случае пожара), автоматического протоколирования несанкционированных изменений в зонах защиты объекта, информирование физической охраны о попытках несанкционированного

доступа. Без обеспечения технической безопасности объем необходимой физической охраны резко возрастает.

Возможности современной техники почти безграничны. Но для того чтобы техническая система безопасности за оптимальные деньги могла решать максимальные задачи, необходимо учесть параметры всех ее элементов. Для крупного или особо важного объекта очень сложно реализовать такую систему при помощи одного или нескольких отдельных технических средств безопасности. Также невозможно обеспечить это только действиями физической охраны. Только комплексный подход позволяет добиться обеспечения безопасности с необходимым уровнем надежности и качества.

Результативная работа всей системы безопасности возможна только при совместной деятельности персонала предприятия, способного осознать все ее аспекты, и руководителей, способных осуществить ее воплощение в жизнь. Необходимы готовность персонала к выполнению требований безопасности, доведение до каждого сотрудника его обязанностей по поддержанию режима безопасности. Необходимо обеспечить службу безопасности надежным инструментарием, а грамотное распределение приоритетов ее деятельности требует участия в ней специалистов, имеющих надлежащую профессиональную подготовку и большой практический опыт.

На сегодняшний день многие коммерческие предприятия не заинтересованы вкладывать приличные средства в то, что не приносит быстрого дохода (в том числе в обеспечение безопасности). Поэтому традиционные системы безопасности сохранят право на жизнь еще на долгие годы, хотя бесспорно, что будущее за интегрированными системами безопасности. Интеграция необходима для повышения эффективности и экономии средств вследствие централизации контроля и управления всеми системами. Простой пример: для внедрения нескольких отдельных систем

безопасности требуется разработать столько же комплектов проектной документации, а для интегрированных систем безопасности необходим всего один. Это графическое изображение (планы объекта с отметками, отражающими состояние отдельных элементов системы). И это возможность получения подробной информации для каждого из элементов на плане или в общей базе данных. Это автоматическая выдача подробных инструкций оператору в ответ на важные события.

Все традиционные системы безопасности в течение долгого периода своего существования развивались самостоятельно, так как они были практически несовместимы между собой. На сегодняшний момент они достигли того уровня, когда их интеграция и возможна, и полезна. Любая из них на данный момент является интегрированной и может сыграть ведущую роль в слиянии остальных систем. В своей основе это все еще замкнутые системы, интегрируемые обычно на основе программного обеспечения с чуть расширенными функциями для поддержки взаимодействия с аппаратурой видеонаблюдения и системами управления зданием, в первую очередь вентиляцией, освещением и кондиционированием. Нередко и системы управления сетевым компьютерным оборудованием встраиваются в программное обеспечение системы безопасности. Немаловажно, что при этом не требуется никакого особенного дополнительного оборудования.

Главный критерий оценки всей системы безопасности – это отсутствие происшествий. Необходимо, чтобы интегрированная система безопасности эффективно отрабатывала нестандартные ситуации, которые, может быть, никогда и не свершатся. Большинство ее основных функций никак не выражаются в обычных ситуациях. Поэтому для проверки работоспособности интегрированных систем безопасности периодически следует проводить специальные учебные тревоги, чтобы оценить реакцию персонала и оборудования, а также выявить их недостатки. А возможность модульного

решения защитных сооружений и конструкций позволяет не только быстро организовать, но и в минимальные сроки адаптировать весь комплекс к изменившейся внешней обстановке.

Оборудовать предприятие интегрированными системами безопасности экономически более выгодно, чем несколькими автономными системами, за счет использования общих линий связи и единых баз данных. Расходы на сервисное обслуживание нескольких мелких систем всегда будут выше, чем на обслуживание одной большой. Но интегрированная система безопасности все-таки является дорогим удовольствием, хотя разработчики и позволяют производить наращивание интегрированной системы безопасности постепенно, растягивая расходы на покупку отдельных модулей. А решение организации системы безопасности другими способами может быть еще дороже. В любом случае целесообразно развернуть на предприятии, по крайней мере, минимальный комплекс технических средств безопасности, который составляет фундамент интегрированной системы безопасности и способен интегрироваться с другими техническими системами. В перспективе такой комплекс позволит наращивать функциональные возможности интегрированной системы безопасности.

Правильный выбор необходимых элементов и производителя технических средств обеспечения безопасности является основополагающим в создании любой современной интегрированной системы безопасности. По мере погружения в технические тонкости той или иной системы проблема выбора только усложняется. Сегодня на рынке технических средств существует значительный разброс цен на принципиально однотипное оборудование. Считается, что выбор элементов интегрированной системы безопасности должен делать сам заказчик, потому что одно и тоже изделие с одинаковыми качествами у разных фирм-производителей может иметь различную стоимость. Но приобретая аппаратуру в «солидных» фирмах, с

устоявшимися традициями и связями с научными (конструкторскими) учреждениями, можно получить сертификат соответствия изделия конкретным требованиям технических условий, и в этих фирмах не обойтись без высоких цен – безопасность стоит дороже.

Обязательно надо провести тщательную маркетинговую проработку существующих технических средств и систем обеспечения безопасности. Возможно, лишний месяц, потраченный на изучение технических характеристик и инструкций, поможет сберечь полгода или больше, которые будут потрачены на запуск и отладку «сырой» системы. Не нужно объяснять, что зачастую интегрированную систему безопасности лучше устанавливать с нуля, чем пытаться скомпоновать старое и новое оборудование.

В области обеспечения безопасности, как и в любой другой, технологии устаревают очень быстро. Наиболее продвинутой характеристикой интегрированной системы безопасности на данный момент является решение не только вопросов безопасности, но и задач по управлению системами жизнеобеспечения здания. Предпочтительно применение оборудования от одного производителя, так как в этом случае есть гарантия, что все элементы будут одинакового класса качества и согласованы по параметрам, что эта система будет работать нормально.

Необходимо отметить, что работоспособные интегрированные системы безопасности появились на нашем рынке лишь несколько лет назад. Импортные технические средства имеют более высокие потребительские характеристики и надежность в эксплуатации, но и с ними может возникнуть целый ряд проблем. Это оборудование может не иметь сертификата, не быть адаптировано к отечественным условиям, а это неизбежно приведет к повышению эксплуатационных расходов при его обслуживании или даже к невозможности его длительной эксплуатации.

Сегодняшним интегрированным системам безопасности еще предстоит долгий путь к полноценному продукту. Но интегрированные системы безопасности на самом деле уже существуют и их можно отнести к разработкам «на перспективу». Но в любом случае грамотному руководителю не стоит забывать, что даже самая дорогая и безупречно экономически обоснованная интегрированная система безопасности себя не оправдает, если ее элементы непрофессионально установлены или настроены. При этом необходимо помнить, что каждая идея (в том числе и система безопасности) может быть доведена до абсурда и понизить эффективность работы предприятия, что она может быть реализована с разными моральными и материальными издержками как для персонала, так и для клиентов.

Итак, для построения интегрированной системы безопасности современного технического уровня не следует:

- применять оборудование, имеющее только локальные функции;

- применять оборудование, не имеющее стандартного цифрового интерфейса для передачи данных и управления функциями;

-применять оборудование и системы, работа которых не может отображаться и управляться стандартными средствами графического интерфейса персонального компьютера;

-применять системы и оборудование, не имеющие четкого технического описания команд и состояний устройств.

Заключение

Известно, что экономическое благополучие и могущество любого бизнеса держится на трех составляющих, имя которым – развитие, безопасность и прибыль.

В современных условиях безопасность бизнеса целесообразно понимать не только как желаемое состояние защищенности от признанных негативными факторов внешней и внутренней среды, но и как процесс адаптации, который постоянно идет внутри бизнеса и подлежит управлению. Структура рассматриваемой в таком свете безопасности предприятия включает сохранение себя (предприятия) как целого, а также своих составляющих – персонала, информации, материальных и нематериальных активов, финансов, клиентуры и, кроме того, своих перспектив развития.

Объектом исследования в магистрской работе является кредитно-финансовая организации «ОАО Банк ВТБ (Азербайджан)». В банке есть служба безопасности, в чьи обязанности, в числе прочих входит работа с кадрами и выявление групп риска. Также внедрен комплекс мер по защите информации. Основным требованием к системе обеспечения собственной безопасности банка является комплексный подход к организации защиты от всех возможных угроз, исключающий наличие незащищенных или плохо защищенных объектов.

При формировании перечня используемых методов защиты от возможных угроз безопасности банка однозначный приоритет должны иметь методы профилактического характера.

Развитие информатики и связанное с этим широкое распространение компьютерных технологий в банковском деле определило расширение перечня возможных угроз как информационной, так и имущественной безопасности кредитно-финансовых организаций. В современных условиях

защита банка от несанкционированного проникновения в его компьютерные сети (для последующего вмешательства в финансовые операции или перехвата информации) стала приоритетной задачей службы безопасности. Основным содержанием деятельности службы безопасности предприятия являются следующие функциональные направления:

1. Своевременное выявление угроз жизненно важным интересам предприятия. При этом основными методами получения информации являются деловая разведка и прогноз-анализ.

2. Предупреждение проникновения (агентурного и технического) к конфиденциальным сведениям (коммерческой тайне) предприятия и обеспечение сохранности информационных ресурсов предприятия. Главными средствами при этом являются: соблюдение охранно-пропускного режима, бдительность сотрудников и технические средства защиты.

3. Обеспечение физической охраны руководства и сотрудников предприятия. При этом основными средствами и методами являются: организация системы упреждающих мер, профессионализм охраняющих и дисциплина охраняемого лица.

С позиции системного подхода безопасность бизнеса должна соответствовать следующим принципам:

- непрерывность - осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности организации. При этом руководители организаций должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала;

- комплексность - использование всех средств защиты финансовых, материальных, информационных и человеческих ресурсов во всех структурных подразделениях организации и на всех этапах ее деятельности;

- своевременность - обеспечение безопасности с использованием упреждающих мер;

- законность - обеспечение безопасности на основе законодательства АР и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции;

- активность - обеспечение безопасности организации с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств;

- универсальность - обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения;

- экономическая целесообразность - сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности должна не превышать размера возможного ущерба от любых видов риска;

- конкретность и надежность - определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом обязательным является достаточное дублирование методов, средств и форм защиты при обеспечении безопасности организации;

- профессионализм - реализация мер безопасности должна осуществляться только профессионально подготовленными специалистами;

- взаимодействие и координация - осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц;

- централизация управления и автономность - обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности бизнеса в целом.

Список использованной литературы:

1. «Sahibkarlıq fəaliyyəti subyektlərinin fəaliyyətinin «bir pəncərə» prinsipi üzrə təşkilinin təmin edilməsi tədbirləri haqqında» Azərbaycan Respublikası Prezidentinin 2007-ci il 25 oktyabr tarixli Sərəncamı.
2. Закон Азербайджанской Республики "Об авторском праве и смежных правах" от 5 июня 1996 г.
3. Закон Азербайджанской Республики «О средствах массовой информации» от 7 дек,1999 г
4. Закон Азербайджанской Республики «О коммерческой тайне» , от 4 декабря 2001
5. Закон Азербайджанской Республики «О правовой охране баз данных» от 14 сентября 2004 года.
6. Закон Азербайджанской Республики "Об информации, информатизации и защите информации" от 3 апреля 1998 г
7. Закон Азербайджанской Республики «О свободе информации» от 19 июня 1998 г.
8. Закон Азербайджанской Республики «О технической безопасности» от 2 ноября 1999 г.
9. Уголовный кодекс Азербайджанской республики от 30декабря 1999 года
10. İqtisadi təhlükəsizlik : dərslik / N. M. Məmmədov, M. İ. Bərxudarov. Bakı : İqtisad Universiteti nəşriyyatı, 2006. - 452 s.
11. Manafov Q.N. «Sahibkarlığın nəzəri və praktiki məsələləri». Bakı, 1997, 144 s
12. Mikayılova S.M. İqtisadi təhlükəsizliyin təmin olunmasının makroiqtisadi problemləri. Monoqrafiya. Bakı, «Gənclik», 2009
13. Əhmədov M. «Milli iqtisadiyyatın iqtisadi təhlükəsizliyi və rəqabət qabiliyyətinin təmin edilməsinin nəzəri səpgiləri» // «İqtisad elmləri: nəzəriyyə və praktika», №3-4. Bakı, 2000, 48-56 s.

14. Sadıqov M.M. «Ölkənin iqtisadi təhlükəsizliyinin qorunmasında maliyyə-kredit mexanizminin rolu» // Azərbaycan Dövlət İqtisad Universitetinin 70 illik yubileyinə həsr edilmiş elmi-praktik konfransın tezisləri. Bakı, 2002

15. Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях./ А.Р. Алавердов. - М.: http://www.e-biblio.ru/cgi-bin/lib.pl

16. Вакуленко Р.Я., Новоселов Е.В. Защита бизнеса и стратегия предприятия: Экономический и правовой аспект. М.: ЮРКНИГА,2005.

17. Гадышев В.А., Поскочинова О.Г. Классификация угроз экономической безопасности предприятия., СПб, 2009

18. Гапоненко В.Ф., Беспалько А.Л., Власков А.С. Экономическая безопасность предприятий. Подходы и принципы. - М.: Издательство «Ось-89», 2007. - 208 с.

19. Гребенников В.В. Стратегия управления экономической безопасностью предприятий. Дис.... канд. эк. наук. Воронеж, 2002.

20. Грибов В.Д. Основы бизнеса. М.Фин. и статистика., 160 с. 2001

21. Захаров О.Ю. Обеспечение комплексной безопасности предпринимательской деятельности. М.-АСТ., ВКТ,2008

22. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. — М.: Новый Юрист, 2008 г.

23. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов . –М.: Горячая линия –Телеком, 2004 . – 280с.

24. Мак-Мак В.П. Служба безопасности предприятия как субъект частной правоохранительной деятельности. Могография. М.; 2004

25. Меламедов С.Л. Формирование стратегии экономической безопасности предпринимательских структур. Дис. Канд. эк. Наук, СПб, 2002.

26. Одинцов А.А. Экономическая и информационная безопасность предпринимательства: учеб.пособие для вузов. – М.:академия, 2008. – 336 с.

27. Соловьев И.Н. Информационная и правовая составляющие безопасности предпринимательской деятельности // Налоговый вес тник. 2002. № 10.

28. Соснин А.С., Прыгунов П.Я. Менеджмент безопасности пред-принимательства: Учеб. пособие. Киев: Изд-во Европ. Ун-та, 2002.

29. Судоплатов А.П., Лекарев С.В. Безопасность предпринимательской деятельности. М.: ОЛМА-ПРЕСС, 2001.

30. Черкасов В.Н. Бизнес и безопасность. Комплексный подход. М.: Армада-пресс, 2001

31. Чумарин И.Г. Внутреннее мошенничество на предприятии - 2. Выявление./ Чумарин И.Г. - М. Опубликовано: БДИ №5/1996 01.05.1996, http://www.poteri.net

32. Ярочкин В.И. Система безопасности фирмы. М.: «Ось-89», 1997.

33. http://www.taxes.gov.az

34. http://www.vtb.az

35. https://www.google.az

36. http://knowledge.allbest.ru

37. http://iti-group.ru

38. http://www.ekb-security.ru/publications

39. http://www.az.all.biz

Xülasə

Tədqiqatın məqsədi– biznesin təhlükəsizliyini təşkiletmə üsüllarının təhlili əsasında müasir biznesin təhlükəsizliyinin təmin edilməsi məsələlərinin həllinə dair elmi cəhətdən əsaslandırılmış təklif və tövsiyələr işləyib hazırlamaqdan ibarətdir.

Dissertasiya işinin məqsədinə çatmaq üçün müvafiq olaraq qarşıya aşağıdakı vəzifələr qoyulmuşdur:

- müasir şəraitdə biznes fəaliyyətinin təhlükəsizliyinə təhdidlərin mahiyyətini müəyyən etmək;

- biznesin təhlükəsizliyinə vahid bir sistem kimi yanaşmaq;

- biznesin təhlükəsizliyinin təmin edilməsinin xarici modellərini öyrənmək;

- biznesin təhlükəsizliyinə dair metodolojı yanaşmaları təsvir etmək;

- bankın timsalında biznesin təhlükəsizliyinin təmin edilməsi məsələlərin təhlili

- biznes fəaliyyətinin təhlükəsizliyinin təşkilində informasiya komponentinin təhlili

- müasir biznesin təhlükəsizlik mexanizmlərinin təkmilləşdirilməsi üçün tövsiyələrin hazırlanması;

Dissertasiya işi üç fəsildən ibarətdir.

Birinci fəsil müasir biznes təhlükəsizliyinin təmin edilməsinin nəzəri-metodoloji əsaslarına həsr edilib.

İkinci fəsildə «Bank VTB (Azərbaycan) ASC» maliyyə-kredit təşkilatın timsalında təhlükəsizliyinin təmin edilməsi məsələləri təhlil edilib.

Magistr işinin üçüncü fəslində müasir biznesin təhlükəsizliyinin təmin edilməsi mexanizminin təkmilləşdirilməsi istiqamətləri göstərilib.

Summary