Кафедра: «Финансы и кредит»

Контрольная работа

Безопасность коммерческого банка

2009

**Вступление**

Само понятие "безопасность" принимает расширенное содержание, оно включает в себя как составляющие информационно-коммерческую, юридическую и физическую безопасность. Вопросы информационно-коммерческой безопасности занимают особое место и в связи с возрастающей ролью информации в жизни общества требуют особого внимания. Успех производственной и предпринимательской деятельности в немалой степени зависит от умения распоряжаться таким ценнейшим товаром, как информация, но выгодно использовать можно лишь ту информацию, которая требуется рынку, но неизвестна ему. Поэтому в условиях ужесточения конкуренции успех предпринимательства, гарантия получения прибыли все в большей мере зависят от сохранности в тайне секретов производства, опирающихся на определенный интеллектуальный потенциал и конкретную технологию.

Понятие "безопасность" определяется как состояние защищенности жизненно важных интересов (Закон РФ "О безопасности"). Однако в общественном сознании все еще сильны стереотипы восприятия безопасности как исключительно относящейся к сфере компетенции государства и специальных органов. Отсюда традиционно "слабое" понимание специфики этих проблем, прежде всего первыми руководителями предприятий и организаций, отнесение ими вопросов информационной безопасности к не основной деятельности. В итоге нередко вопросы защиты коммерческой тайны упускаются в лицензионных соглашениях, договорах подряда на создание научно-технической продукции. Такие упущения приводят к утечке коммерчески значимой информации, затрудняют определение собственника на результаты работы.

Переход экономики на рыночные отношения, в том числе и в вопросах интеллектуальной собственности, требует от руководителей предприятий не только разработки рыночной стратегии, но и стратегии информационной безопасности, в том числе специальной программы по защите интеллектуальной собственности, определения подразделений и лиц, ответственных за проведение на предприятии данной работы.

Такая программа должна преследовать две основные цели: обеспечение защиты уже наработанных объектов интеллектуальной собственности, имеющих коммерческую ценность, и предотвращение утраты таких объектов в будущем. При этом следует отметить, что в отличие от организации секретного делопроизводства, данная работа должна проводиться значительно более гибко при соответствующей патентно-информационной и юридической проработке.

**1. Какая информация относится к коммерческой тайне?**

Систему российского законодательства, регулирующего отношения, связанные с коммерческой тайной, образуют правовые нормы различных отраслей права: конституционного, гражданского, уголовного и административного. Общие нормы содержит Конституция РФ. Она закрепляет и гарантирует право каждого на предпринимательскую деятельность, право на информацию, а также на защиту своих прав и свобод.

Центральные источники права, регулирующие отношения, связанные с коммерческой тайной, занимают Гражданский кодекс и Федеральный закон «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ с изменениями от 2008 года, а также вступившая в силу с 1 января 2008 года IV часть Гражданского кодекса. Понятие коммерческой тайны отождествляется с секретом производства (ноу-хау). Федеральный закон «О коммерческой тайне» регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности, а также определяет сведения, которые не могут составлять коммерческую тайну.

Когда говорят о коммерческой тайне, речь идет о конфиденциальной информации, которая позволяет ее обладателю увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг, т.е. получить коммерческую выгоду.

А информация, составляющая коммерческую тайну, - это научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства), которая обладает следующими признаками:

* имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
* сведения получены легитимно, то есть имеют законное происхождение;
* к ней нет свободного доступа на законном основании;
* обладателем такой информации введен режим коммерческой тайны в отношении нее и предприняты все меры для сохранения конфиденциальности.

Кроме того, логично, что  к коммерческой тайне может быть отнесена только документированная информация, то есть зафиксированная на каком-либо материальном носителе. Идеи, замыслы, сведения и прочие данные остаются незащищенными, если они не зафиксированы в материальной форме.

В новой редакции закона «О коммерческой тайне» есть уточнение о том, что к информации, составляющей коммерческую тайну (секрет производства) относятся сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности.

Закон определяет только признаки, которыми должна обладать информация для отнесения ее к коммерческой тайне. Однако Закон содержит перечень сведений, которые не могут составлять коммерческую тайну. К ним относятся сведения, которые объективно должны быть открытыми и общедоступными (учредительные документы, сведения о регистрации, о работниках, о безопасности объектов).

Для того чтобы информация могла считаться коммерческой тайной, она должна иметь действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам. Во-первых, под коммерческой ценностью понимается способность информации быть объектом рыночного оборота. Во-вторых, к коммерческой тайне относится информация, использование которой предоставляет её обладателю определённые экономические преимущества в силу того, что его конкуренты такой информацией не обладают. Если же информация не представляет экономической ценности, она не может считаться коммерческой тайной. К коммерческой тайне относятся сведения, представляющие интерес для третьих лиц, которые могли бы получить определённую выгоду, если бы они этой информацией обладали. В-третьих, информация, составляющая коммерческую тайну, может иметь потенциальную коммерческую ценность, т.е. знания и сведения, которые не используются, но могут быть использованы в будущем.

Руководители бизнес-структур коммерческой тайной обычно считают следующее:

* сведения о персонале, персональные данные работников;
* любые сведения, которые сообщил клиент;
* данные о структуре издержек, себестоимости, бюджете, планах на будущее;
* технологии работы;
* стратегические и тактические решения, способствующие эффективному развитию бизнеса, получению конкурентных преимуществ, бизнес-проекты;
* маркетинговые технологии, и, в частности, оценку эффективности рекламных коммуникаций;
* сведения о технических средствах и системах защиты информационных ресурсов;
* базы данных и систематизированные информационные массивы.

Закон выдвигает два принципиальных, но в чем-то противоречивых требования. С одной стороны, должен быть исключен "доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя", а с другой стороны, необходимо обеспечить "возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны". Но в крупной компании это серверы баз данных, приложений, электронной почты, файл-серверы. И на каждом из них есть информация, составляющая коммерческую тайну. Сетевые администраторы, администраторы серверов, администраторы безопасности, пользователи обычные и привилегированны. Разграничить доступ так, чтобы и режим не нарушить, и обеспечить при этом возможность нормально функционировать бизнес-процессу, не остановив его окончательно очень не просто.

Нельзя относить к коммерческой тайне сведения, прямо запрещенные Законом. Для всех остальных сведений ограничений на отнесение нет, но следует постоянно помнить, что информация становится способной к правовой охране в качестве коммерческой тайны, если только она действительно обладает коммерческой ценностью и к ней нет свободного доступа на законном основании. И это тоже создает сложности. Вполне разумно отнести к коммерческой тайне сведения о доходах работников. Но как обязать работника хранить их в тайне и как в таком случае должна выглядеть выдаваемая ему на руки форма 2-НДФЛ? Ответы на эти вопросы - скорее отрицательные. А значит, и информацию отнести к коммерческой тайне нельзя - режимные меры для нее практически невыполнимы. И это только один возможный пример.

Без помощи владельцев бизнес-процессов и юристов при составлении перечня информации, составляющей коммерческую тайну, никак не обойтись. И поэтому серьезной ошибкой является распространенная практика возложения разработки перечня на службу безопасности. Не может она это сделать - ни по уровню квалификации, ни по самому смыслу, вкладываемому в перечень.

**2. Мероприятия по защите информации**

Всех уже перестал удивлять тот факт, что в продаже постоянно появляются сведения, составляющие коммерческую тайну той или иной  организации. Сегодня не составит труда приобрести клиентскую базу или персональные данные работников интересующей вас компании. Это происходит потому, что руководители организаций не прилагают достаточных усилий для защиты информации, относящейся к коммерческой тайне. Более того, не стоит забывать о реально существующих охотниках за подобной информацией. Научно-технический прогресс внес в нашу жизнь большое количество технических средств, позволяющих производить запись телефонных переговоров, совещаний, появилась возможность считывать информацию с экрана компьютера, территориально находясь вне места расположения компании.

Но основным источником утечки информации являются сотрудники. Именно они «сливают» информацию, составляющую коммерческую тайну. Причин тому может быть масса – и получение дополнительного заработка, и по неосторожности или случайно.

На сегодняшний день компании, специализирующиеся на технической защите ценной информации, предлагают ряд продуктов, способных осуществлять динамическую блокировку устройств, через которые злоумышленники могут скачать информацию.

Но против человеческого фактора защиту строить сложнее. Необходимо четко разъяснить сотрудникам, какая информация относиться к коммерческой тайне, и какова степень ответственности за ее разглашение. Ограничьте доступ к информации, составляющей коммерческую тайну: определите порядок обращения с этой информацией, осуществляйте контроль за соблюдением такого порядка. Разработайте специальную инструкцию по соблюдению конфиденциальности.

В обязательном порядке необходимо  заключить с работниками  трудовые договоры, а с контрагентами (лат. contrahens — договаривающийся — лица, учреждения, организации, связанные обязательствами по общему договору, сотрудничающие в процессе выполнения договора) гражданско-правовые договоры, в которых должны содержаться условия об охране конфиденциальной информации. Обязательство о неразглашении коммерческой тайны может быть составлено в любой форме, важно чтобы оно содержало перечень сведений, которые в вашей компании составляют коммерческую тайну.

Также организовать специальное делопроизводство, обеспечивающее  сохранность носителей, содержащих коммерческую тайну, и внедрите систему разъединения информации по блокам. Каждый сотрудник должен знать ровно столько, сколько необходимо для выполнения его обязанностей.

Еще одним способом защиты прав обладателя коммерческой тайны является установление санкций за нарушение обязательств по соблюдению конфиденциальности контрагентами в гражданско-правовых договорах. По общему правилу, защита нарушенных гражданских прав осуществляется в судебном порядке (признание права, пресечение незаконных действий, возмещение убытков). Кроме гражданско-правовых способов защиты, коммерческая тайна может быть защищена по нормам трудового, уголовного права, а также по нормам о недобросовестной конкуренции.

Из возможностей, предусмотренных трудовым правом, права обладателя коммерческой тайны могут защищаться такими действиями как привлечение к материальной ответственности и привлечение к дисциплинарной ответственности вплоть до прекращения трудовых отношений. Кроме того, при наличии признаков правонарушения, предусмотренных соответствующими отраслями права, возможно, привлечение правонарушителей к уголовной ответственности.

При хранении информации в электронном виде можно выделить три направления работ по защите информации: теоретические исследования, разработка средств защиты и обоснование способов использования средств защиты в автоматизированных системах.

В теоретическом плане основное внимание уделяется исследованию уязвимости информации в системах электронной обработки информации, явлению и анализу каналов утечки информации, обоснованию принципов защиты информации в больших автоматизированных системах и разработке методик оценки надежности защиты.

К настоящему времени разработано много различных средств, методов, мер и мероприятий, предназначенных для защиты информации, накапливаемой, хранимой и обрабатываемой в автоматизированных системах. Сюда входят аппаратные и программные средства, криптографическое закрытие информации, физические меры организованные мероприятия, законодательные меры. Иногда все эти средства защиты делятся на технические и нетехнические, причем, к техническим относят аппаратные и программные средства и криптографическое закрытие информации, а к нетехническим - остальные перечисленные выше.

### а) аппаратные методы защиты.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

-специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности,

-генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства,

-устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации,

-специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты,

-схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

### б) программные методы защиты.

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения функций защиты и включаются в состав программного обеспечения систем обработки данных. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п. По функциональному назначению их можно разделить на следующие группы:

-идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей,

-определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей,

-контроль работы технических средств и пользователей,

-регистрация работы технических средств и пользователей при обработки информации ограниченного использования,

-уничтожения информации в ЗУ после использования,

-сигнализации при несанкционированных действиях,

-вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

### в) резервное копирование.

Резервное копирование информации заключается в хранении копии программ на носителе. На этих носителях копии программ могут находится в нормальном (несжатом) или заархивированном виде. Резервное копирование проводится для сохранения программ от повреждений (как умышленных, так и случайных), и для хранения редко используемых файлов.

### г) криптографическое шифрование информации.

Криптографическое закрытие (шифрование) информации заключается в таком преобразовании защищаемой информации, при котором по внешнему виду нельзя определить содержание закрытых данных. Криптографической защите специалисты уделяют особое внимание, считая ее наиболее надежной, а для информации, передаваемой по линии связи большой протяженности, - единственным средством защиты информации от хищений.

Основные направления работ по рассматриваемому аспекту защиты можно сформулировать таким образом:

-выбор рациональных систем шифрования для надежного закрытия информации,

-обоснование путей реализации систем шифрования в автоматизированных системах,

-разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем,

-оценка эффективности криптографической защиты.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований, в том числе: достаточная стойкость (надежность закрытия), простота шифрования и расшифрования от способа внутримашинного представления информации, нечувствительность к небольшим ошибкам шифрования, возможность внутримашинной обработки зашифрованной информации, незначительная избыточность информации за счет шифрования и ряд других. В той или иной степени этим требованиям отвечают некоторые виды шифров замены, перестановки, гаммирования, а также шифры, основанные на аналитических преобразованиях шифруемых данных.

Особенно эффективными являются комбинированные шифры, когда текст последовательно шифруется двумя или большим числом систем шифрования (например, замена и гаммирование, перестановка и гаммирование). Считается, что при этом стойкость шифрования превышает суммарную стойкость в составных шифрах.

Каждую из систем шифрования можно реализовать в автоматизированной системе либо программным путем, либо с помощью специальной аппаратуры. Программная реализация по сравнению с аппаратной является более гибкой и обходится дешевле. Однако аппаратное шифрование в общем случае в несколько раз производительнее. Это обстоятельство при больших объемах закрываемой информации имеет решающее значение.

### д) физические меры защиты.

Следующим классом в арсенале средств защиты информации являются физические меры. Это различные устройства и сооружения, а также мероприятия, которые затрудняют или делают невозможным проникновение потенциальных нарушителей в места, в которых можно иметь доступ к защищаемой информации. Чаще всего применяются такие меры:

-физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений,

-ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточны для исключения эффективной регистрации электромагнитных излучений, и организации систематического контроля этих территорий,

-организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудованных входных дверей специальными замками, позволяющими регулировать доступ в помещения,

-организация системы охранной сигнализации.

### е) организационные мероприятия по защите информации.

Следующим классом мер защиты информации являются организационные мероприятия. Это такие нормативно-правовые акты, которые регламентируют процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется. Организационные мероприятия играют большую роль в создании надежного механизма защиты информации. Причины, по которым организационные мероприятия играют повышенную роль в механизме защиты, заключается в том, что возможности несанкционированного использования информации в значительной мере обуславливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью пользователей или персонала систем обработки данных. Влияние этих аспектов практически невозможно избежать или локализовать с помощью выше рассмотренных аппаратных и программных средств, криптографического закрытия информации и физических мер защиты. Для этого необходима совокупность организационных, организационно-технических и организационно-правовых мероприятий, которая исключала бы возможность возникновения опасности утечки информации подобным образом.

Основными мероприятиями в такой совокупности являются следующие:

-мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров (ВЦ),

-мероприятия, осуществляемые при подборе и подготовки персонала ВЦ (проверка принимаемых на работу, создание условий при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности за нарушение правил защиты),

-организация надежного пропускного режима,

-организация хранения и использования документов и носителей: определение правил выдачи, ведение журналов выдачи и использования,

-контроль внесения изменений в математическое и программное обеспечение,

-организация подготовки и контроля работы пользователей,

Одно из важнейших организационных мероприятий - содержание в ВЦ специальной штатной службы защиты информации, численность и состав которой обеспечивали бы создание надежной системы защиты и регулярное ее функционирование.

Таким образом, рассмотренные выше средства, методы и мероприятия защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

**Список использованных источников**

1. В.И. Ярочкин Безопасность банковских систем / Ярочкин В.И. – М.: Ось-89, 2004.- 416 с.
2. Стрельченко Ю.А. Организация защиты коммерческой тайны предприятия / Ю.А. Стрельченко – М.: Контроллинг, 2002.- 268 с.
3. Гражданский кодекс РФ от 18.12.2006 г. № 230-ФЗ Часть четвертая.
4. Болдырев Ю.Н., Матвеева С.Р., Торговая газета // Методический журнал «О коммерческой тайне» - 2006. - № 56.
5. Федеральный закон Российской федерации от 29 июля 2004 г. № 98 – ФЗ «О коммерческой тайне», с изменениями от 2008 г.
6. www@rg.ru – электронная версия Российской газеты