



## **ВВЕДЕНИЕ**

Обеспечение безопасности является неотъемлемой составной частью деятельности организации. Состояние защищенности представляет собой умение и способность надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам организации.

Объектами безопасности являются:

- персонал (руководство, ответственные исполнители, сотрудники);
- финансовые средства, материальные ценности, новейшие технологии;
- информационные ресурсы.

Главной целью системы безопасности является обеспечение устойчивого функционирования организации и предотвращение угроз его безопасности, защита законных интересов от противоправных посягательств, охрана жизни и здоровья персонала, недопущение хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утечки и несанкционированного доступа к служебной информации, нарушения работы технических средств обеспечения производственной деятельности, включая и средства информатизации.

В современных условиях персонал предприятия необходимо рассматривать как самостоятельный объект защиты от различных угроз. Это определяется рядом факторов, отражающих имущественные и неимущественные интересы работодателя. Так, часть сотрудников предприятия в силу занимаемой должности является носителями конфиденциальной информации, которая несет опасность разглашения. Не меньшую угрозу представляет для работодателя потеря ценных для него кадров из числа руководителей и ведущих специалистов.

### Глава 1. Персонал как объект защиты

Дополнительная актуальность защиты собственного персонала связана с действием следующих факторов:

- большой удельный вес сотрудников, выступающих как носителей информации, составляющей коммерческую тайну;
- более высокая степень профессиональной специализации и технологической обособленности труда служащих, что создает дополнительные проблемы при необходимости оперативного замещения внезапно освободившихся рабочих мест.

Типовой перечень потенциальных угроз персоналу:

- прямое переманивание конкурентами ведущих руководителей и специалистов;
- вербовка сотрудников конкурирующими и криминальными структурами, а в отдельных случаях – правоохранительными органами;
- шантаж или прямые угрозы в адрес конкретных сотрудников с целью склонения их к нарушению доверия со стороны работодателя (т.е. к совершению различных должностных нарушений);
- покушения на сотрудников (прежде всего, высших руководителей банка) и членов их семей.

Перечень категорий сотрудников как объектов защиты (ранжированный по степени приоритетности):

- высшее руководство банка (президент и его первые заместители);
- главные специалисты и эксперты по конкретным направлениям деятельности (финансы, маркетинг, компьютерные технологии и т.п.);
- сотрудники, занимающие рабочие места, предполагающие доступ к особо конфиденциальным сведениям (стратегические планы развития, обслуживание элитных клиентов, организация систем безопасности и т.п.);
- прочие сотрудники.

## **Глава 2. Организация защиты от возможной угрозы шантажа, пути решения**

Защита от шантажа и угроз в адрес сотрудников в современных условиях основными предметами шантажа в адрес сотрудников являются (в ранжированном виде):

- уже допущенные сотрудниками нарушения доверия работодателя (хищения, коррупция, разглашение конфиденциальной информации и т.п.);
- факты и обстоятельства, способные скомпрометировать в глазах работодателя личностные или профессиональные качества сотрудника (образ жизни, хронические заболевания, постоянные контакты и т.п.);
- факты и обстоятельства, способные стать причиной претензий к сотруднику со стороны правоохранительных органов (административные или уголовные правонарушения) или налоговых служб;
- факты и обстоятельства, способные стать причиной угроз благополучию личной жизни сотрудника (с учетом изменившихся морально-этических норм поведения – в современных условиях наименее вероятно).

Наряду с традиционными методами служб безопасности и персонала по контролю над общей лояльностью сотрудников, основным методом профилактики подобных угроз является разъяснение им:

- техники шантажа как одного из инструментов угроз безопасности;
- типовых ситуаций, при которых шантаж может стать возможным;
- правил поведения в случае шантажа (при этом четко излагается основной тезис: «если объект шантажа, ранее действительно нарушивший доверие работодателя, немедленно ставит об этом в известность службу безопасности, то он либо полностью освобождается от ответственности, либо несет ее в минимально возможном объеме»).

После того, как факт шантажа установлен, служба безопасности может в зависимости от общей стратегии своей деятельности использовать различные методы пресечения:

- самостоятельно или через шантажируемого сотрудника довести до субъекта угрозы информацию об ее выявлении (наиболее простой метод, рекомендуемый для банков, проводящих стратегию пассивной защиты);
- в случае выявления факта шантажа без участия его объекта либо сразу уволить шантажируемого сотрудника, либо «втемную» использовать его как источник дезинформации субъекта угрозы (вариант, рекомендуемый для банков, проводящих стратегию адекватного ответа);

- использовать добровольно признавшегося сотрудника в качестве источника дезинформации субъекта угрозы (вариант, требующий дополнительных гарантий личной безопасности участвующему в операции сотруднику).

В отличие от шантажа, прямые угрозы в адрес сотрудников чаще всего не связаны с негативными моментами в их профессиональной деятельности или личной жизни. Основным критерием выбора объекта угроз является должностное положение сотрудника и возможности, которые из него вытекают. Лишь в случае, когда целям субъекта угрозы могут способствовать одновременно несколько служащих, на его выбор могут повлиять их личные качества, например, нерешительность, боязнь любых открытых конфликтов, любовь к семье и т.п.

Субъектами подобных угроз чаще всего выступают:

- криминальные структуры (в основном из категории «молодых группировок», обычно не представляющие серьезной опасности для банка из-за ограниченных возможностей);

- собственные сотрудники, заинтересованные в сокрытии информации о допущенных нарушениях (обычно либо прямые руководители объекта угрозы, либо начальники инспектируемых им подразделений).

Основным методом профилактики является разъяснение сотрудникам банка необходимости немедленного информирования службы безопасности о факте угрозы, высказанной в любой форме. При этом до сведения обучаемого доводятся:

- полная бесперспективность для субъекта практической реализации угрозы, если о ней уже стало известно работодателю;

- возможности службы безопасности по защите от подобных угроз;

- возможность получения объектом угроз, оперативно оповестившим службу безопасности, специальных компенсационных выплат или социальных льгот (естественно, при подтверждении реальности такой угрозы).

Для подтверждения факта угроз служба безопасности может использовать разнообразные технические средства и оперативные мероприятия, в рамках, регламентированных действующим законодательством.

Пресечение дальнейших угроз осуществляется различными методами, в зависимости от избранной стратегии обеспечения собственной безопасности:

- увольнение или иные санкции к своему сотруднику, допустившему угрозы в адрес подчиненного или ревизора;
- оповещение правоохранительных органов;
- решение проблемы с внешним для банка субъектом угрозы иными, не противоречащими закону методами.

## **Заключение**

Борьба с шантажом – комплексная задача. Здесь, как правило, эффект дают совместные действия сотрудников различных служб, в том числе подразделений собственной безопасности, одна из задач которых – обеспечение безопасности сотрудников в ходе их профессиональной деятельности, а также защита системы от недобросовестных сотрудников. Наряду с проведением правовых и организационных мероприятий одним из путей решения этой проблемы является обучение сотрудников, особенно молодых, тактике и методам защиты от шантажа, провокаций и контрдействиям в этой ситуации.

Под шантажом подразумевается манипулятивный способ воздействия, в процессе которого субъекта (сотрудника) ставят перед выбором: либо он выполнит все требования шантажирующего, либо порочащая его информация будет предоставлена определенным лицам.

### Список использованной литературы

1. Алавердов А. Управление кадровой безопасностью организации: Учебник / Академическая серия – М.: Изд. МАРКЕТ-ДС, 2008.
2. Гамза В.А., Ткачук И.Б. Концепция и система безопасности банка. – М.: Издатель Шумилова И.И., 2003.
3. Организация и современные методы защиты информации / Подред. А.Гиеваи А.Шаваева–М.: «Банковский деловой центр», 1998.
4. Закон РФ «О безопасности» от 05.03.1992.
5. Закон РФ «О частной детективной и охранной деятельности в РФ» от 11.03.1992.
6. Закон РФ «Об информации, информатизации и защите информации» от 20.02.1995.