Лекционный материал на тему

«**Работа по обучению персонала, допускаемому к конфиденциальной информации**»

Текущая работа с персоналом, владеющим конфиденциальной информацией, включает в себя:

· Обучение и систематическое инструктирование сотрудников;

· Проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;

· Постоянный контроль за выполнением персонала требований по защите конфиденциальной информации;

· Контрольную работу по изучению степени осведомленности персонала в области конфиденциальных работ организации;

· Проведение служебных расследований по фактам утечки информации и нарушений персоналом требований по защите информации;

· Совершенствование методики текущей работы с персоналом.

Процесс обучения сотрудников правилам защиты информации должен быть постоянным, так как система защиты требует регулярного обновления и видоизменения.

Обучение сотрудника начинается с момента проведения собеседования с ним при приеме на работу и подписания им обязательства о не разглашении и заканчивается моментом увольнения и подписания этим лицом обязательства о недопустимости использования конфиденциальных сведений в чьих-либо целях.

Задачи обучения включают изучение:

· Характера и состава конфиденциальной информации;

· Возможных угроз конфиденциальным сведениям, каналов их объективного распространения и каналов утраты, методов работы злоумышленников;

· Структуры системы защиты, требований и правил защиты конфиденциальной информации;

· Порядка работы сотрудников с конфиденциальными сведениями, документами и базами данных;

· Действий персонала в конкретных экстремальных ситуациях.

Обучение предполагает приобретение и поддержание на высоком уровне производственных навыков работы с конфиденциальными сведениями, психологическое воспитание сотрудников и воспитание глубокой убежденности в необходимости выполнения требований по защите любой конфиденциальной информации.

Методика обучения включает в себя:

· Специализированные программы обучения для обеспечения лекционных курсов и практических занятий;

· Проведение лекций, семинаров и собеседований;

· Решение ситуационных задач;

· Практическую ситуационную учебу по действиям персонала в экстремальных ситуациях;

· Проведение деловых игр, обучающих методам противодействия замыслам злоумышленников.

Одновременно с обучением должны проводиться регулярные совещания-инструктажи с сотрудниками, в процессе которых до них доводятся изменения и дополнения в нормативно-методические документы по защите информации; также сотрудники информируются о конкретных угрозах информации, каналах утечки, принятых мерах, анализируются случаи нарушения правил защиты информации.

Здоровый психологический климат в коллективе создает барьер на пути любого злоумышленника, которые пытается получить конфиденциальную информацию.

Процесс обучения и воспитания сотрудников организации должен завершаться контролем работы персонала с конфиденциальной информацией и документами. Важен контроль защиты ценной информации от недобросовестных посягательств отдельных сотрудников.

Регулярный и своевременный учет состава конфиденциальной информации, известной каждому из сотрудников, является наиболее информативной частью контрольной работы. Учитываются любые контакты любого сотрудника с конфиденциальными сведениями, в т.ч. санкционированные, а также случайные.

Традиционная (карточная) или электронная учетная форма должна содержать ряд предметных зон, позволяющих сопоставлять функциональные обязанности сотрудника и состав конфиденциальной информации, полученной сотрудником, который должен соответствовать выполняемым видам работы. В **учетную форму включены такие зоны**:

· Зона штатных функциональных обязанностей сотрудника, при реализации которых используется конфиденциальная информация;

· Зона изменений и дополнений, внесенных в функциональные обязанности сотрудника, с указанием документа-основания, его даты и фамилии руководителя, подписавшего документ;

· Зона стандартного состава конфиденциальных сведений и их индексов, к которым допущен сотрудник в соответствии с должностной инструкцией;

· Зона изменений и дополнений в составе конфиденциальных изменений и их индексов по перечню, к которым допускается сотрудник в связи с пересмотром его должностных обязанностей;

· Зона документированной информации, с которой знакомится или работает сотрудник, с указанием наименований документов, их дат и номеров, краткого содержания, целевого использования сведений и их индексов по перечню, фамилии руководителей, разрешивших работу с документами;

· Зона недокументированной конфиденциальной информации, которая стала известна сотрудника, с указанием даты и цели ознакомления, фамилии руководителя, разрешившего ознакомление, состава конфиденциальных сведений и их индексов по перечню;

· Зона обнаруженного несанкционированного ознакомления сотрудника с конфиденциальной информацией с указанием даты ознакомления, условий и причин ознакомления, фамилия виновного сотрудника, места ознакомления, состава конфиденциальных сведений и их индексов по перечню.

Анализ осуществляется сравнением содержания записей в зонах и индексов известной сотруднику конфиденциальной информации, т.е. ведется поиск несоответствия.

Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в т.ч. в части защиты информации, можно назвать следующие:

· Аттестация сотрудников;

· Отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;

· Регулярные проверки руководителем или службой безопасности соблюдения сотрудниками требований по защите информации;

· Самоконтроль сотрудников.

Аттестация сотрудников – одна из наиболее эффективных форм контроля деятельности сотрудников, как в профессиональной сфере, так и в сфере соблюдения информационной безопасности организации. Аттестация - это коллективная форма оценки профессиональной пригодности сотрудника, его соответствия занимаемой должности. Аттестация проводится периодически. По результатам аттестации издается приказ, в котором отражаются решения аттестационной комиссии о поощрении, переаттестации, повышении в должности или увольнении сотрудников. Комиссия может также выносить решение об отстранении сотрудника от работы с конфиденциальной информацией.

Одна из форм контроля – заслушивание руководителей структурных подразделений и руководителя службы безопасности о состоянии системы выполнении ее требований сотрудниками подразделений.

Другая форма контроля – регулярные проверки выполнения сотрудниками правил работы с конфиденциальными документами. Проверки проводятся руководителями структурных подразделений, замами первого руководителя, работниками службы безопасности. Проверки могут быть как плановыми, так и внеплановыми (внезапными).

При работе с персоналом следует сосредоточивать внимание не только на сотрудниках, работающих с конфиденциальной информацией. Под контролем должны находиться также лица, не имеющие доступа к тайне организации.

В случае установления фактов невыполнения сотрудниками требований по защите информации к ним должны применяться меры порицания и наказания в соответствии с правилами внутреннего трудового распорядка: объявление выговора, понижение в должности, лишение премии, отстранение от работы с конфиденциальной информацией, увольнение.

Факт утраты информации выявляется в основном посредством анализа публикаций, рекламы, выставочных и других материалов фирм-конкурентов. В этом случае анализируются карточки учета осведомленности сотрудников в тайне организации и выявляется круг сотрудников, владеющих утраченной информацией. Анализ ведется в рамках служебного расследования.

Служебное расследование организуется по фактам разглашения или утечки информации, утраты документов и изделий, другим грубым нарушениям правил защиты информации. Расследование ведется специально сформированной комиссией. Расследование предназначено для выяснения причин, всех обстоятельств и их последствий, связанных с конкретным фактом установления круга виновных лиц, размера причиненного организации ущерба. Все мероприятия документируются.

Расследование проводится в кратчайшие сроки. В ходе его обычно анализируются следующие виды документов:

· Письменные объяснения опрашиваемых лиц;

· Акты проверки документации и помещений, где указываются фамилии лиц, проводивших проверку, их должности, объем и виды проведенного осмотра, результаты, указываются подписи этих лиц, дата;

· Другие документы, относящиеся к расследованию (справки, заявления, планы, анонимные письма и т.д.).

По результатам анализа составляется заключение о результатах проведенного расследования, в котором подробно описывается проделанная работа, указываются причины и условия случившегося, определяются виновные лица, даются рекомендации по предотвращению в будущем подобных фактов. Вопрос о наказании виновных лиц ставится после завершения расследования. При подтверждении факта передачи сотрудником информации постороннему лицу фирма должна обратиться в суд для вынесения решения о возмещении материального ущерба от кражи информации.