Переподготовка менеджеров по ИБ на текущем месте, насколько часто рекомендуется и почему это важно.

1. Важность и необходимость развития системы менеджмента в информационной безопасности.

В последнее время большую известность приобрела проблема информационной безопасности. Информационная безопасность играет важную роль в обеспечении жизненно важных интересов не только страны, но и конкретно отдельного предприятия. Создание развитой и защищенной информационной среды является обязательным условием развития каждой компании.

Последнее время в мире происходят качественные изменения в процессах управления на всех уровнях, обусловленные интенсивным внедрением современных информационных технологий. Параллельно возрастает опасность несанкционированного вмешательства в работу информационных и телекоммуникационных систем. Весомость возможных последствий такого вмешательства для предприятия возросла настолько, что наиболее важные подразделения организации стали в максимальной степени зависимыми от уязвимости своих информационных систем. Именно поэтому в последнее время в этих организациях все большее внимание уделяется проблемам защиты информации и поиску путей их решения.

В эпоху развития информационных технологий, с каждым годом все больше и больше растет число утечек конфиденциальной информации, совершенных случайно или по оплошности персонала. Одной из причин этого является низкий уровень квалификации сотрудников компании. Перед украинскими предпринимателями стоит непростая задача оптимизировать затраты предприятия и сохранить высокий уровень безопасности, в том числе и информационной. Без повышения квалификации персонала, такую задачу решить будет очень сложно.

Практика последних лет показывает, что подготовка специалистов в области информационной безопасности становится не только актуальной, но и жизненно необходимой для существования предприятия. Риски для компании, связанные с различными воздействиями на ее информационную инфраструктуру, являются неотъемлемой частью процесса управления непрерывностью бизнеса в организации. Традиционные методы и средства обеспечения информационной безопасности требуют дальнейшего совершенствования, привязки к изменяющимся условиям.

Как правило, особенно в предприятиях с небольшим количеством сотрудников, в вопросах защиты информации руководители полагаются на рядовых сотрудников, не имеющих соответствующей квалификации. Другие же руководители считают, что справиться с задачей обеспечения информационной безопасности предприятия сможет практически любой специалист, знакомый с информационной технологией, способный настроить любую вычислительную технику, установить необходимые программы и средства. Однако большая часть проблем в области информационной безопасности не решается только путем применения программно-аппаратных средств. Умение взглянуть на проблему защиты информации и обеспечения информационной безопасности в целом требует от сотрудников не только знания технологий, но и менеджерских навыков в данной области.

По мнению специалистов, ввиду того, что возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловлены не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты, важную роль в создании надежного механизма защиты информации играют **организационные мероприятия**.

К ним можно отнести:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений;
- мероприятия, осуществляемые при подборе персонала;
- организация и поддержание надежного пропускного режима, охраны помещений и территории, контроля за посетителями;
- организация хранения и использования документов и носителей конфиденциальной информации;
- организация защиты информации;
- **организация регулярного обучения сотрудников.**

2. Для чего необходима переподготовка менеджеров по ИБ на текущем месте?

Анализ состояния защиты информации в предприятиях свидетельствует о том, что в целом решение этой проблемы далеко от совершенства.

Организация должна гарантировать, что весь персонал, которому доверена защита информации, компетентен в этом направлении и готов для выполнения требуемых задач.

Прежде всего, руководитель должен перед собой видеть ряд задач необходимых для повышения информационной безопасности, а именно:

- определять необходимый уровень компетентности персонала, выполняющего работу, связанную с информационной безопасностью;
- обеспечивать подготовку соответствующего персонала или нанимая на работу уже подготовленных специалистов, с целью удовлетворения этой потребности;
- поддерживать на высоком уровне компетенцию персонала, его опыт и мастерство в вопросах информационной безопасности.

Кроме того, руководитель организации должен проводить внутренние аудиты системы информационной безопасности с целью определения:

- соответствия Системы требованиям защиты информационной безопасности;
- соответствия уровня профессиональной подготовки специалистов информационной безопасности современным требованиям защиты информации;
- эффективности использования всех средств безопасности и поддержания их в исправном (рабочем) состоянии;
- полноты выполнения задач и целей управления, состояния средств управления, процессов и процедур системы информационной безопасности.

Все эти мероприятия, в конце концов, сводятся к одному – важному месту менеджера в системе информационной безопасности, его компетентности и мастерстве при выполнении задач по защите информации.

Более того, современный специалист по информационной безопасности должен уметь определять состав защищаемой информации, ее ценность, степень уязвимости, рассчитывать ущерб от возможной потери информации, оценивать качество и эффективность различных методов и средств защиты. Он должен уметь проводить специальные исследования и сертификацию различных технических средств обработки информации, ориентироваться в отечественном и зарубежном рынке средств информационной безопасности, проектировать и внедрять системы ИБ, знать и использовать зарубежный опыт.

Новичок этот менеджер или специалист с опытом, с целью приобретения вышеперечисленных навыков, он требует регулярной подготовки в вопросах информационной безопасности, изучения современных средствах выявления источников утечки информации, их использования и совершенствования навыков в борьбе со злоумышленниками.

Без дальнейшего развития менеджмента в области информационной безопасности, работы в этом – стратегически важном направлении, развитие организации просто может полностью утратить свою целесообразность и эффективность.

3. Как часто необходима переподготовка менеджеров по ИБ на текущем месте?

Одним из Принципов формирования и проведения государственной политики в сфере Технической защиты информации (ТЗИ), согласно Концепции защиты информации в Украине, является обеспечение подготовки специалистов для роботы в сфере ТЗИ.

Задача подготовки высококвалифицированных специалистов решается в рамках системы подготовки, переподготовки и повышения квалификации в области информационной безопасности и защиты информации.

Государственные и коммерческие структуры активно занимаются подготовкой и переподготовкой сотрудников, занимающихся в этой сфере деятельности. Большинство контрагентов рынка придерживается убеждения, что специалисты в области информационной безопасности должны проходить переподготовку **не реже 2 раз в год**, с тем, чтобы поддерживать профессиональное соответствие в условиях быстро развивающихся информационных технологий и, как следствие, усложняющихся методов киберпреступности.

Учебные программы, разработанные за последние годы различными учебными центрами, призваны помочь руководителям в решении данной проблемы.

Все зависит от конкретного профиля компании. Для одних главной задачей является предотвращение утечки информации к конкурентам. Для других – это целостность информации. Для третьих компаний важной считается задача безотказной работы информационных систем.

Ввиду того, что с информационной безопасностью связаны не только менеджеры по ИБ, процесс обучения специалистов в этой области условно можно разделить на подготовку руководителей и подготовку сотрудников, ответственных за эту деятельность в компании.

Учебные программы могут представлять собой как 2-х-3-х дневные практические семинары, так и длительные курсы продолжительностью в несколько недель. Последний вариант не всегда требует полного отрыва сотрудника, направляемого организацией на обучение, от исполнения непосредственных рабочих обязанностей, поскольку занятия могут проводиться в определенные дни по вечерам. Очевидно, что эффективность работы сотрудников, обеспечивающих безопасность информационных систем, напрямую зависит от уровня их подготовки и наличия соответствующего опыта работы. Все это происходит на фоне повышения осведомленности каждого сотрудника компании в вопросах информационной безопасности.