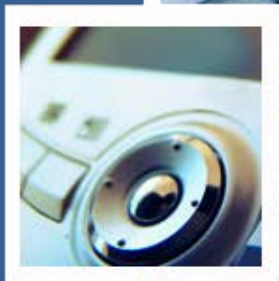


Информационная безопасность

На службе
бизнеса



Причины низкой эффективности подразделений ИБ



- Информационная безопасность в 90% случаев входит в состав Служб безопасности, Управления Рисками или Служб внутреннего контроля.
- Отсутствие квалифицированных кадров в сфере ИБ.
 - Бывший сотрудник внутренних органов, осуществляющий мониторинг или реже администрирование DLP, PUM, CCTV и СКУД.
 - Аудитор-теоретик – контролирующий выполнение IT-подразделением исполнения предписаний регулятора или внешнего аудитора.
- Фактической защитой инфраструктуры IT занимаются сетевые, системные и DBA администраторы.
- Применение только технических средств в качестве инструментов ИБ (DLP, Firewall, сканеры, пентестеры и т.д.). Без «творческого подхода» к задаче.

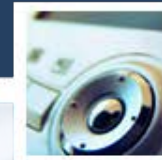
Сферы применения ИБ



- Финансовый сектор содержит штат «информационной безопасности» без особого понимания его необходимости, но по требованию регулятора. А действительный же функционал по защите инфраструктуры возлагается на IT подразделения.
- Собственник негосударственной коммерческой структуры не готов содержать штат или развивать направление ИБ, при таком сомнительном профите. А большая часть специалистов ИБ, на данный момент не могут предложить спектр услуг, который бы его заинтересовал.

У меня есть мечта...

(Мартин Лютер Кинг)



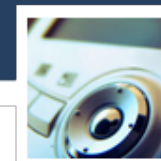
- Объединение в подразделении ИБ функционала:
 - Экспертов сетевой инфраструктуры,
 - IT-аналитиков,
 - IT-аудиторов,
 - СЕН-специалистов,
 - Data грабберов,
 - Конкурентной разведки
 - Контр разведки

Участие IT в реализации стратегических задач



№	Тактическая задача	Роль IT подразделения	Комментарии
1	Снижение операционных расходов, увеличение оборота и маржинальности, повышение продаж с квадратного метра	Вспомогательная	Поддержка операционных и коммерческих подразделений. Автоматизация бизнес-процессов
2	Сокращение издержек на содержание IT инфраструктуры, повышение ее рентабельности	Основная	Поиск, оценка, вынесение на рассмотрение и внедрение IT инструментов. Постоянная оптимизация IT инфраструктуры
3	Эффективный анализ продаж, планирование закупок, контроль остатков; ценообразования и логистических процессов;	Основная	Обеспечение корректности данных учетных систем и алгоритмов BI инструментов. Полное и своевременное предоставление данных.
4	Предотвращение противоправных действий, хищений, незаконных вознаграждений	Вспомогательная	Поддержка и техническое обеспечение
5	Приобретение конкурентного преимущества путем накопления уникальных знаний, специалистов, эксклюзивных договорных отношений и иных ноу-хау. А так же их защита.	Вспомогательная	Поддержка и техническое обеспечение

ИБ – активный инструмент бизнеса



№	Тактическая задача	Роль ИТ подразделения	Комментарии	Роль подразделения ИБ
1	Снижение операционных расходов, увеличение оборота и маржинальности, повышение продаж с квадратного метра	Вспомогательная	Поддержка операционных и коммерческих подразделений. Автоматизация бизнес-процессов	Контроль расходов ИТ, участие в выборе ИТ стратегии развития, применения технологий. Проведения тендеров и закупок. Контрольный и надзорный орган ИТ. Альтернативное мнение.
2	Сокращение издержек на содержание ИТ инфраструктуры, повышение ее рентабельности	Основная	Поиск, оценка, вынесение на рассмотрение и внедрение ИТ инструментов. Постоянная оптимизация ИТ инфраструктуры	
3	Эффективный анализ продаж, планирование закупок, контроль остатков; ценообразования и логистических процессов;	Основная	Обеспечение корректности данных учетных систем и алгоритмов BI инструментов. Полное и своевременное предоставление данных.	Извлечение и фундаментальный анализ информации об активности и деятельности конкурентов и, а так же около отраслевое изучение событий. Во результате данных действий могут быть скорректированы управленческие решения.

ИБ – активный инструмент бизнеса



№	Тактическая задача	Роль IT подразделения	Комментарии	Роль подразделения ИБ
4	Предотвращение противоправных действий, хищений, незаконных вознаграждений	Вспомогательная	Поддержка и техническое обеспечение	Содействие подразделению экономической и внутренней безопасности. Сбор информации, выявление семантических связей, мониторинг ключевых сотрудников и контрагентов.
5	Приобретение конкурентного преимущества путем накопления уникальных знаний, специалистов, эксклюзивных договорных отношений и иных ноу-хау. А так же их защита.	Вспомогательная	Поддержка и техническое обеспечение	Ведение информационного противостояния с конкурирующими организациями. Установление источников интереса, контроль их шагов и действий. Дезинформация и превентивные меры.

Статистика

