

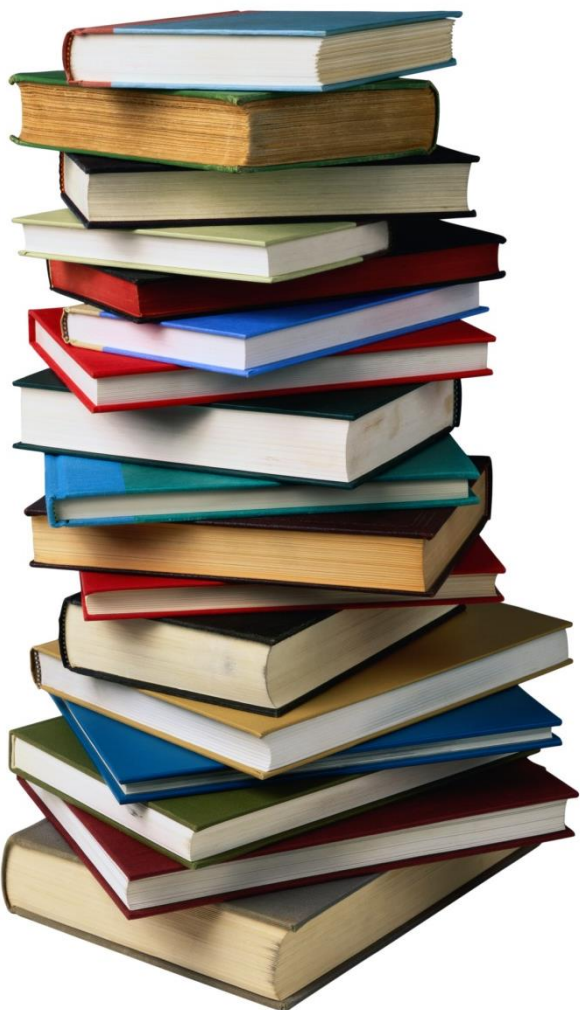
Программа повышения осведомленности персонала в области информационной безопасности

Автор: Уваровская О.Б.

Докладчик: Уваровская О.Б.

Руководитель: Шулик А.А.





- ✓ ГОСТ Р ИСО/МЭК 27001-2006
«Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
- ✓ Федеральный закон от 27.06.2006г. № 152-ФЗ
«О персональных данных»
- ✓ Политика информационной безопасности ОАО «Газпром» (утверждена приказом ОАО «Газпром» от 15.02.2008г. №48).

Цель программы повышения осведомленности



Основная цель – минимизировать количество инцидентов информационной безопасности, вызванных неправильными действиями сотрудников.



Распределение ошибочных ответов сотрудников по категориям



1. Обучение

2. Рассылка

**3. Плакаты/
ЛИСТОВКИ**

**4. Неделя повышения
осведомленности**

**5. Регулярная
проверка уровня
осведомленности**

1. Обучение

Цель – рассказать сотрудникам компании :

- ✓ об обязанностях и ответственности в области ИБ
- ✓ о существующих угрозах и рисках для информации
- ✓ о преимуществах выполнения правил по ИБ

Средства обучения:
семинары, презентации,
электронная система
обучения



2. Рассылка

Цель рассылки – постоянно напоминать сотрудникам компании о принятых правилах информационной безопасности



Средства рассылки –
электронная почта,
мессенджер Spark

3. Плакаты и листовки

Цель плакатов и листовок – «незаметно» заставить сотрудников задуматься об информационной безопасности



Цель – привлечь внимание сотрудников к проблеме информационной безопасности в организации

Средства – семинары, рассылка, плакаты, шуточная электронная игра



Паранойя – важный инструмент в усилении информационной безопасности сотрудников Компании (а еще профессиональная болезнь специалистов по информационной безопасности)

ЯВНИВАЮЩУ МИЛЛИОН ДОЛЛАРОВ

Каждое письмо по электронной почте должно быть проверено на наличие вирусов и вредоносных программ. Если вы получили письмо от незнакомца, не открывайте его, не отвечайте и не сообщайте никому о его содержании. Если вы получили письмо от знакомого, но оно выглядит подозрительно, сообщите об этом в службу информационной безопасности.

Самое сложное в работе специалиста по ИБ - определить, сколько документов отправить на согласование юристам...

Меня заинтересовала ваша вакансия Эксперта по информационной безопасности. Вот мой резюме, оно переведено на английский, закодировано и пропущено через шредер."

Наш секретный пароль состоит из 6 частей

Чтобы узнать их необходимо решить ряд типовых задач Специалиста по ИБ

1. Разрабатывать документы по ИБ
2. Расследовать инцидент
3. Повысить паранойю коллег
4. Организовать проблемы с сетью

Задания воспользуемся Хитрым генератором случайных чисел:

И генератор выдает число 26 (двадцать шесть),
и, что должны отправить на согласование 13 документов

И генератор выдает число 22 (двадцать два),
то должны отправить в ЮД 11 документов на согласование

Хитрый генератор выдает число 100 (сто),
и должны отправить в итоге не 50 документов. А сколько?
Сколько?

Или мы будем писать письма коллегам
вместо наших писем компьютеру будет писать
число расписок: сделать уровень паранойи более 80
на
имя
Я знаю, что Вы делали прошлым летом!
Эффективность отправки 4

5. Проверка уровня осведомленности

Цель – узнать реальный уровень осведомленности сотрудников в вопросах информационной безопасности

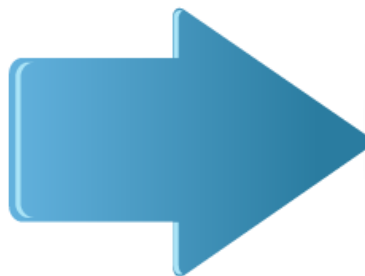
Средства – тестирование, опросы, проверки, количество инцидентов



5. Проверка уровня осведомленности



Электронное письмо
с просьбой перейти
по сомнительной
ссылке



13%
сотрудников
перешли по
ссылке

Уважаемые коллеги!

Открывая подозрительные ссылки, полученные от неизвестных людей, Вы рискуете попасть на сайты, содержащие вредоносное программное обеспечение (вирусы), запрещенный законодательством контент или сайты-подделки известных служб и сервисов (почта, социальные сети и прочее).



P.S. Очень жаль, что все мои лекции и рассылки прошли зря, жду Вас на ближайшем семинаре по информационной безопасности!

С уважением, специалист по обеспечению режима коммерческой тайны.

Страничка с напоминанием о
необходимости соблюдения правил
информационной безопасности

**Безопасность информации в компании
зависит от каждого из нас!**



**Благодарю
за внимание!**