18 февраля 2016, Магнитогорск

Информационная безопасность в НФО: примеряем СТО-БР

Гольдштейн Анна,

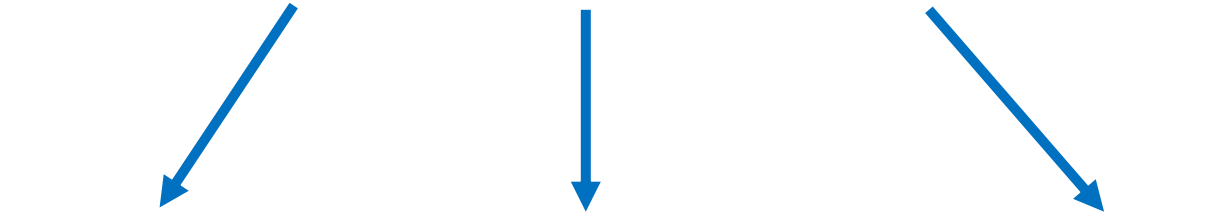
Директор по развитию бизнеса

ЗАО НИП «Информзащита»

Маленькая прелюдия

Эффект от стандартизации

Возможный результат:



Цель стандартизации?

Информзащита
Системный интегратор

20 лет

Задачи

- ✓ Оценка рисков ИБ и разработка минимально необходимого набора мер для закрытия идентифицированных рисков;
- ✓ Формулирование этого набора требования в форме MUST HAVE
- ✓ Разработка рекомендаций (Best practices) по реализации этого набора требований (отраслевой опыт) – видоизменяемая часть, наиболее часто обновляемая

Информзащита
Системный интегратор
20 лет

Анализ потенциальной эффективности

Формулировки «требований»

- Нечеткие (< = > нет требования);
- Смешаны требования и лучшие практики;
- Избыточные / неэффективные;
- Просто непонятные.

Примеры «требований»

- Нечеткие (< = > нет требования)

«7.6.10 В НФО РФ должны быть определены состав и порядок использования мер защиты, применяемых при взаимодействии с сетью Интернет и позволяющих обеспечить противодействие атакам злоумышленников..»

- Смешаны требования и лучшие практики

«блокирования сеанса доступа после установленного времени бездействия и (или) по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации (например, после трех неуспешных попыток доступа) для продолжения работы (блокировка компьютера во время бездействия или отсутствия работника на рабочем месте)»

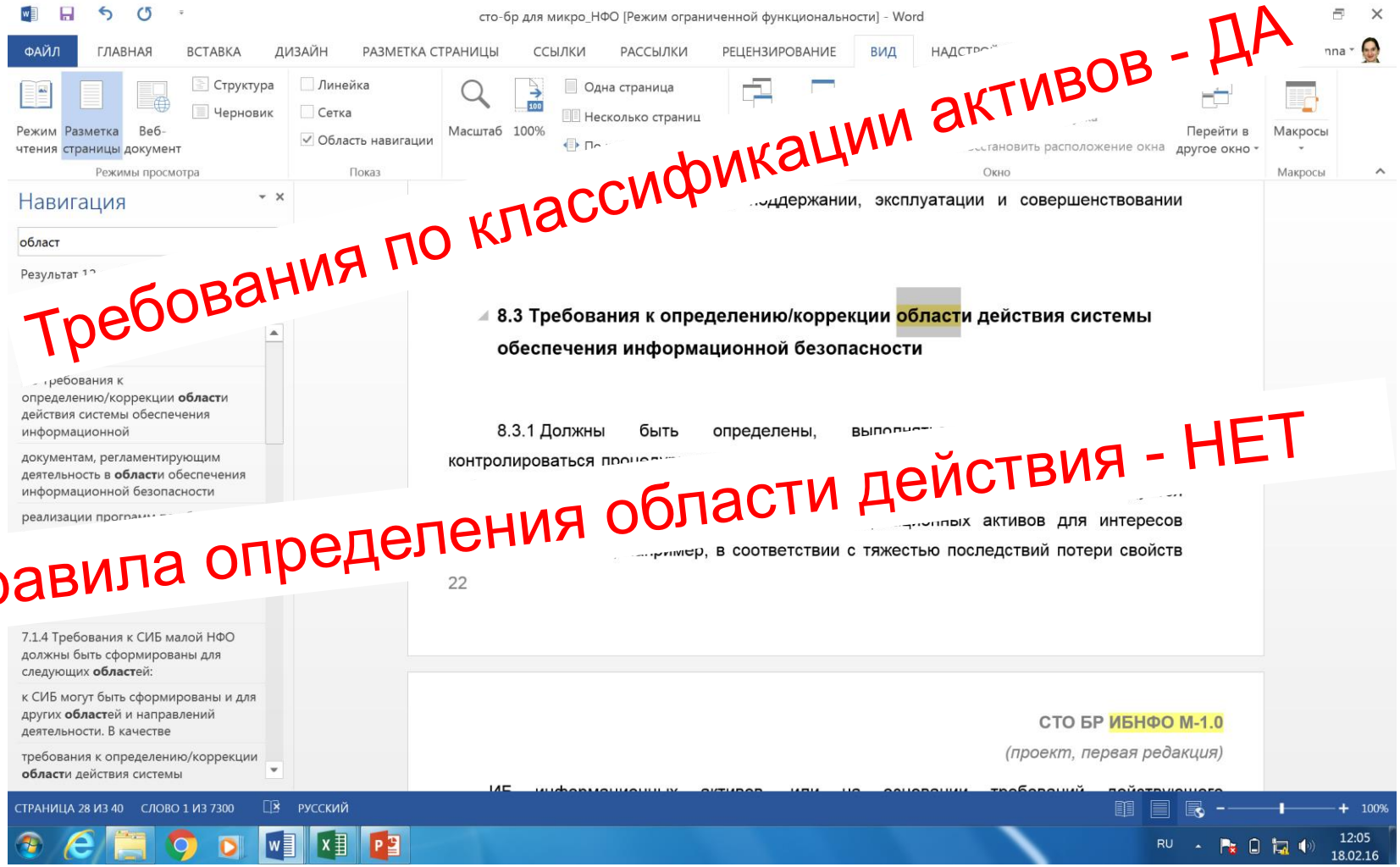
- Избыточные/неэффективные

«7.6.11 В документах организации должно быть установлено положение, устанавливающее запрет на самостоятельную загрузку работниками свободно распространяемого или условно бесплатного программного обеспечения из сети Интернет. Такая загрузка допускается только по решению руководства малой НФО и осуществляться под контролем уполномоченного за обеспечение ИБ.»

- Просто непонятные

«8.1.3 Этап «реализация» выполняется по результатам выполнения этапов «планирование» и (или) «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование» и (или) реализации решений, определенных на этапе «совершенствование» и не требующих выполнения деятельности по планированию соответствующих улучшений. В том числе важным является выполнение таких видов деятельности, как организация обучения и повышение осведомленности в области ИБ, реализация обнаружения и реагирования на инциденты ИБ, обеспечение непрерывности бизнеса НФО РФ.»

Область применения СОИБ (SCOPE)



ЕГЭ 2016 по информатике

Контрольный тест

Где действует система обеспечения ИБ?

(Выберите ОДИН правильный ответ)

- ☐ везде
- ☐ нигде

Информзащита
Системный интегратор

20 лет

Состав СИБ и оценка рисков

«*Набор требований к СИБ может быть изменен*»:

- Сокращен или расширен (НФО)
- Уточнен или расширен (малое НФО)

- «*…Банк России является сторонником регулярной оценки уровня ИБ в НФО РФ, оценки риска нарушения ИБ и принятия мер, необходимых для управления этим риском.*»

Информзащита
Системный интегратор
20 лет

Зачем оценка рисков тем, кто не пытается обосновать право не выполнять базовые требования СИБ?

Информзащита
Системный интегратор

20 лет

Методика оценки: почувствуйте разницу!

Документы	Реализация	Оценка
-		0
+	-	0,25
+	+-	0,5
+	++-	0,75
+	+	1

Информзащита
Системный интегратор

20 лет

Ресурсное обеспечение

СИБ

- Контроль доступа
- Защита от НСД и НРД
- Антивирусная защита
- Контроль использования ресурсов сети Интернет
- СКЗИ
- Безопасность АС на стадиях ЖЦ

СМИБ

- Разработка/поддержание нормативной документации
- Повышение осведомленности по ИБ
- Мониторинг/реагирование на инциденты ИБ
- Контроль реализации защитных мер

Информзащита
Системный интегратор
20 лет

Резюмируя…

- Область применения стандарта не определена;
- Набор «базовых» мер (раздел 7) на практике неизменяемый, оценка рисков зачастую является профанацией;
- Применяемая практика методики оценки степени соответствия СТО-БР приводит к избыточной документированности в ущерб реализации;
- Выполнение требований СТО-БР для НФО (особенно для малых) требует неадекватных ресурсов. Принципы привлечения аутсорсинга ИБ для этих целей не определены;
- Форма изложения требования стандарта позволяет их свободное толкование (значит, уход от обязательности выполнения), трудна для понимания.

Предложения

Область действия:

- Определение критериев обязательного включения в область действия (по существу конкретных бизнес-процессов, виду обрабатываемой информации, значимости для сохранения собственного капитала организации,..);
- Критерии – специфичны для разного вида деятельности организаций, относимых к НФО.

Оценка рисков и определение защитных мер:

- Требовать только для обоснования отказа от применения требований к СИБ 7 раздел.

Методика оценки:

- Перенести акцент с документированности на выполнение установленного требования.

Информзащита
Системный интегратор
20 лет

Предложения – часть 2

Ресурсное обеспечение и аутсорсинг ИБ:

- Определить правила привлечения третьей стороны и переноса ответственности за защищенность активов

Форма:

- Разделение текста на стандарт + рекомендации по реализации стандарта
- Существенная переработка формулировок + исключение методики оценивания из текста требований (определено ли, выполняется и контролируется..)

Информзащита
Системный интегратор
20 лет

Спасибо.
Вопросы?

Гольдштейн Анна
goldanna@infosec.ru