**Методика организации и проведения деловой игры**

**«Построение модели угроз информационной безопасности для малого предприятия»**

**Деловая (ролевая) игра** – эффективный метод взаимодействия обучающихся. Она является формой моделирования тех систем отношений, которые существуют в реальной действительности или в том или ином виде деятельности, в них приобретаются новые методические навыки и приемы.

Деловая игра – метод имитации принятия решений руководящих работников или специалистов в различных производственных ситуациях, осуществляемый по заданным правилам группой людей или человеком с информационной системой в диалоговом режиме, при наличии конфликтных ситуаций или информационной неопределенности.

*Цель деловой игры*: Анализ эффективности системы информационной безопасности (ИБ) организации с использованием аппарата моделирования с полным перекрытием множества угроз (программный инструментарий прилагается) с привлечением *Специалистов отдела ИТ*, *Специалистов отдела защиты информации* и *Экспертов-аналитиков по ИБ*.

*Роли участников игры:*

**Специалисты отдела ИТ** (3-4 человека)

При проектировании или оценки эффективности существующей системы защиты информации, чрезвычайно важно, чтобы различные конфликтные ситуации между сотрудниками службы ИТ и специалистами отдела защиты информации разрешались в форме продуктивного диалога.

Задачи специалистов отдела ИТ в данной деловой игре.

1. Подготовить для специалистов отдела защиты информации материалы по потенциальным угрозам ИБ, перечню инцидентов ИБ и прочие материалы, необходимые для анализа и построения модели ИБ в организации. Для достижения поставленной цели специалисты отдела ИТ должны проанализировать структуру объекта оценки (*Приложение 1*) и подготовить ответы на вопросы (*Приложение 4*) для специалистов отдела защиты информации и экспертов-аналитиков.
2. Провести совместное совещание со специалистами отдела защиты информации (ЗИ) с целью анализа ответов на вопросы (*Приложение 4*) и формирования полного множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.
3. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.

**Специалисты отдела защиты информации** (3-4 человека)

Одной из задач специалистов по защите информации является оценка эффективности существующей в организации системы ИБ. Для решения этой задачи необходимо проводить интервью со специалистами ИТ с целью выявления слабостей в системе защиты информации, анализа инцидентов ИБ и подготовки материалов для построения модели: *угрозы-средства защиты-объекты оценки*.

Задачи специалистов отдела ЗИ в данной деловой игре.

1. Запросить у специалистов ИТ опросники (*Приложение 4*), помочь в заполнении опросников и проконсультировать ИТ-специалистов в случае возникновения неоднозначных ситуаций
2. Проанализировать полученные из отдела ИТ опросники (внести дополнительные сведения, при необходимости). На основании изучения описания организации (*Приложение 1*) и опросника, полученного от специалистов ИТ (*Приложение 4*), заполнить формы анализа угроз ИБ (*Приложение 5*) для передачи экпертам-аналитикам
3. Провести совместное совещание со специалистами отдела ИТ с целью формирования множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.
4. Передать скорректированные тексты экспертам-аналитикам (*Приложение 3*) и внести сведения в базу данных.
5. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.

**Эксперты-аналитики в области ИБ** (2 человека)

Сведения по множествам угроз безопасности; объектам оценки и средствам защиты информации на предприятии поступают к экспертам-аналитикам в области ИБ с целью их анализа, корректировки, построения модели угрозы-средства защиты-объекты защиты и анализу полученной модели.

Задачи экспертов-аналитиков в области ИБ в данной деловой игре.

1. Изучить инструкцию пользователя по работе с программным обеспечением для построения модели с полным перекрытием множества угроз (*Приложение 2*) и подготовить программу к использованию.
2. Проанализировав сведения (*Приложения 1, 3, 4*), внесенные в базу данных специалистами ЗИ, скорректировать данные (после проведения совместного совещания со специалистами ИТ и ЗИ).
3. Построить модель с полным перекрытием множества угроз ИБ (описание работы с программным обеспечением в *Приложении 2*)
4. Проанализировать полученную модель и сделать выводы по повышению эффективности системы ИБ в организации.
5. Собрать итоговое совещание со специалистами ИТ и ЗИ, где огласить выводы и обсудить дальнейшие мероприятия по повышению эффективности системы защиты информации в рассматриваемой организации.

Подведение итогов, подробный анализ деловой игры:

* общая оценка игры, подробный анализ реализации целей и задач, удачные и слабые стороны, их причины (проводится преподавателем);
* самооценка участниками исполнения полученных заданий, степень личной удовлетворенности (оценки сотрудникам службы ИТ и ЗИ выставляют руководители этих служб, назначенные перед началом игры; оценка деятельности экспертов по ИБ проводится преподавателем);
* характеристика профессиональных знаний и умений, выявленных в процессе игры (проводится преподавателем);

Критерием оценок может служить количество и содержательность выдвинутых идей (предложений), степень самостоятельности суждений, их практическая значимость. Оценивание осуществляется по десяти бальной шкале.

*Литература*

1. Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие. – М.: Изд. Центр ЕАОИ, 2010. – 376 с.
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР: ИНФРА-М, 2014. – 256 с.
3. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум. - М.: РИОР: ИНФРА-М, 2015. – 161 с.
4. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности. ж.”Управление риском”– М., 2009.– № 1(49).– С.15-26.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб.пособие для вузов – М.: Горячая линия – Телеком, 2004.- 280 с.
6. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов СВ.- М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.