# Практическая работа № 4

**Тема: Разработка политики безопасности организации.**

**Цель:** Получение студентами опыта разработки политики безопасности организации.

**Краткая теория**

**Политика безопасности (ПБ**)– совокупность документированных решений, принимаемых руководством организации для защиты информации, отражающих подход организации к защите своих информационных активов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации.

ПБ верхнего уровня – решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации.

ПБ среднего уровня – вопросы, касающиеся отдельных аспектов (сторон) ИБ, но важные для различных систем, входящих в организацию.

ПБ нижнего уровня относится к конкретным информационным сервисам.

Таблица 2 – Инструкционная карта деловой игры

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Этап игры** | Время | **Деятельность участников игры** | Задание | Результат работа на этапе |
| Подготовительный - формулируется цель игры и дается необходимая информация | 7 минут | Группа делится на команды по 4-6 чел. | 1. Разделиться на группы 2. Записать тему занятия 3. Ответить на вопросы преподавателя | 1. Записана тема занятия |
| 1 этап – распределение ролей в группах | 8 минут | Каждая группа представляет собой команду руководства банка. В руководство банка входят:  1. Директор банка,  2. Директор по безопасности (начальник службы охраны)  3. Директор по персоналу  4. Директор по IT,  5. Юрисконсульт (помощник по юридическим вопросам).  В руководство организации при необходимости могут быть включены другие специалисты (директор по финансовым вопросам, начальник вычислительного центра или ведущий инженер-программист). | 1. Выбрать название организации (банка) 2. Записать название банка на табличке, которая находится на столе 3. Распределить роли между участниками | 1. Табличка с названием банка 2. Список сотрудников банка |
| 2 этап – самостоятельная работа студентов в командах | 30 минут | Руководство банка должно провести совещание, на котором будет выработана политика безопасности организации для защиты своих информационных активов.  Для определения стратегии защиты необходимо:  1. Провести анализ рисков для информационной системы организации  2. Сформулировать политику безопасности банка. Она должна быть представлена в виде программы. | 1. Провести анализ рисков для информационной системы организации 2. Выявить риски, которые показали максимальный обобщенный ущерб 3. Сформулировать предложения по уменьшению эти рисков 4. Сформулировать политику безопасности банка в виде программы. | 1. Таблица «Анализ рисков» 2. Список мер по снижению основных рисков 3. Политика безопасности верхнего уровня |
| 3 этап - самостоятельная работа студентов в группах | 20 минут | Учебная группа делится по другому признаку - объединение происходит по должности. Задача каждой группы – разработать политику безопасности нижнего уровня для своего отдела.  Директора банков в это время оформляют политику безопасности верхнего уровня в электронном виде. | 1. Провести совещание отдела и сформулировать политику безопасности нижнего уровня для своего отдела, т.е. план по защите информации 2. Директорам банков оформить политику безопасности верхнего уровня в электронном виде (презентация). | 1. Программа по защите информации в отделе (политика безопасности нижнего уровня) 2. Презентация «Политика безопасности верхнего уровня» |
| 4 этап - анализ решений, подведение итогов деловой игры | 20 минут | Директора банков защищают свои программы. Зачитываются программы нижнего уровня.  Представитель каждого отдела защищает свою программу – политику безопасности нижнего уровня | 1. Директора банков представить свои программы, ответить на вопросы оппонентов 2. Представителям каждого отдела представить программу нижнего уровня своего отдела. 3. Все участники деловой игры задают уточняющие вопросы. | 1. Директора защищают свои проекты 2. Представитель каждого отдела защищает свою программу 3. Оценка работы групп на 1-2 этапе 4. Оценка работы групп на 3 этапе |
| 5 этап - рефлексия | 3 минуты | Студенты заполняют небольшой опросник | Заполнить опросник | 1. Заполненная анкета |

# Критерии оценивания

Второй и третий этап оцениваются отдельно. Все участники деловой игры, кроме тех, кто выбрал для себя должность директора, получают по 2 оценки за работу в группе.

Участники группы получают одинаковую оценку.

Таблица 3 - Критерии оценивания этапов 1- 2:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № группы | Проверка выполнения задания 1  (максимальное количество - 15 баллов) | | | | | | Защита проекта (максимальное количество – 5 баллов) | | |
| Выбрано название банка (2 балла) | Распределены роли (1 балл) | Выполнен анализ рисков ИС организации (5 баллов) | Приведены меры для снижения вероятности основных угроз (3 балла) | Составлена политика безопасности банка (3 баллов) | Политика безопасности не имеет грубых ошибок (2 балла) | Качество презентации (2 балла) | Убедительность аргументов(2 балла) | Ответы на вопросы оппонентов(1 балл) |
| 1 |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |

Максимальная оценка за этап – 20 баллов.

Таблица 4 – Таблица для подсчета общего количества баллов за этапы 1-2:

|  |  |  |
| --- | --- | --- |
| Количество баллов | | Оценка |
| 18-20 | | 5 |
| 14-17 | | 4 |
| 11-13 | | 3 |
| меньше 11 | | 2 |
|  |  | |

Оценка за урок \_\_\_\_\_\_\_\_\_\_\_\_

Таблица 5 - Критерии оценивания этапа 3:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № группы | Проверка выполнения задания 2  (каждый критерий – 1 балл) | | | | | | |
| Все участники вовлечены в работы (2 балла) | Представлена программа по защите информации (2 балла) | Программа имеет не менее 6 пунктов (2 балла) | | Программа имеет комплексный характер (2 балла) | Качество аргументов и защиты программы (1 балл) | Ответы на вопросы оппонентов( 1 балл) |
| 1 |  |  |  |  | |  |  |
| 2 |  |  |  |  | |  |  |
| 3 |  |  |  |  | |  |  |
| 4 |  |  |  |  | |  |  |
| 5 |  |  |  |  | |  |  |

Максимальная оценка за этап – 10 баллов

Таблица 6 – Таблица для подсчета общего количества баллов за этап 3:

|  |  |  |
| --- | --- | --- |
| Количество баллов | | Оценка |
| 9-10 | | 5 |
| 7-8 | | 4 |
| 5-6 | | 3 |
| меньше 5 | | 2 |
|  |  | |

Оценка за урок \_\_\_\_\_\_\_\_\_\_\_\_

*После выполнения практической работы* ***студент должен:***

*иметь практический опыт:*

* разработки политики безопасности организации;
* разработки политики безопасности нижнего уровня;

*уметь:*

* анализировать риски информационной безопасности для конкретной организации;

*знать:*

* правовые меры обеспечения информационной безопасности;
* организационные меры обеспечения информационной безопасности;

программно-технические меры обеспечения информационной безопасности.