**Конкурсное задание**

**по презентационной компетенции**

**40 Информационная безопасность**

 **автоматизированных систем**

Задание рассчитано на 3 дня, состоит из пяти модулей и охватывает следующие технологии:

* модуль A - Построение модели угроз безопасности и разработка основных положений политики безопасности организации (50 баллов);
* модуль B - Использование встроенных механизмов разграничения доступа ОС Windows (20 баллов);
* модуль C - Использование возможностей ОС Windows по криптографической защите информации (5 баллов);
* модуль D - Использование возможностей ОС Windows по обеспечению сохранности информации(10 баллов);
* модуль E - Использование USB-токенов ( eToken ) для повышения защищенности ОС Windows (15 баллов).

*Первый день.*

 **Модуль A – Построение модели угроз безопасности и разработка основных положений политики безопасности организации**

*Время выполнения* – 5 часов

*Вводные данные:*

Строительно-монтажная компания «Х» имеет занимает 2-й этаж двухэтажного здания, схема представлена на рис.

 

 

Офис компании предназначен для осуществления управления предприятием, проведение совещаний и переговоров.

 Стены объекта выполнены из кирпичной кладки, толщина кладки 2 кирпича, внутренние стены так же выполнены из кирпича, толщина кирпичной кладки составляет 1 кирпич. На объекте защиты установлены окна с двойным остеклением, с толщиной стекла 3 мм.

 Вход на объект расположен в центральной части здания и оборудован металлическими дверями.

 Освещение объекта электрическое. Электропроводка по стенам проложена в пластиковых кабель-каналах, за подвесными потолками в пластиковых трубах.

 В здании смонтированы и находятся в рабочем состоянии следующие инженерные системы: отопления; холодного и горячего водоснабжения; вентиляции и кондиционирования воздуха; Оконные конструкции во всех помещениях охраняемого объекта остеклены.

Офис оснащен:

Система электропитания (освещение) галогенные потолочные светильники (6 шт.).

Система заземления: имеется.

Система вентиляции (тип): приточно-вытяжная, с мех. побуждением, проем 250\*160 мм.

Система отопления:

- центральное водяное: водяное, три стояка, проходящие транзитом снизу вверх
- наличие экранов на батареях: декоративное укрытие.

Телефонные линии:

- количество и тип ТА - 2 шт., ( Voice Coder-2400- 1 шт), Panasonic - беспроводной 900 МГц )

- городская сеть 1 шт., два параллельных аппарата (обычный и беспроводной)

- тип розеток: евророзетка.

- тип проводки: двухпроводные линии.

 Офис компании автоматизирован. Компания занимается строительством объектов промышленного и гражданского назначения, ведет монтаж технологического оборудования, инженерных сетей и сооружений. Среди партнеров компании присутствуют крупнейшие заводы-производители металлопроката, поставщики железобетонных изделий и конструкции, что позволяет с успехом конкурировать на рынке строительных услуг.

 В составе организации имеется внутренняя служба технического надзора, которая ведет тщательный контроль за процессом строительства, в связи с чем, деятельность организации соответствует высоким стандартам качества. Кроме этого, имеется своя служба безопасности, которая обеспечивает, как информационную безопасность офиса, так и безопасность строительных объектов, технический отдел, кадровый отдел, работающий с персональными данными сотрудников.

 Компания обратилась к вам как специалисту в области информационной безопасности для построения модели угроз и разработки политики безопасности организации.

*Выходные данные:*

Выходными данными при выполнении задания 1-го модуля являются следующие документы, которые составляет каждый участник соревнований:

1. Модель угроз безопасности
2. Основные положения политики безопасности организации

Задача участника – провести анализ угроз информационной безопасности, составить модель угроз и сформулировать основные положения политики безопасности организации.

1. Анализ уязвимостей (подготовительный этап)

Анализ уязвимостей — необходимый этап в создании эффективной системы безопасности. По его результатам составляются модели угроз и разрабатываются проектные варианты технических комплексов безопасности.

Анализ уязвимости объекта информатизации проводится с целью определения возможных последствий воздействия нарушителей на элементы объекта, оценки показателей уязвимости объекта (эффективности охраны), выявления слабых мест и недостатков существующей системы охраны или рассматриваемых проектных вариантов системы, а в итоге — выбора наилучшего варианта системы охраны для конкретного объекта.

Анализ уязвимости объекта включает:

А) разработку модели нарушителей;

Б) выделение и категорирование особо важных зон объекта;

В) оценку показателей уязвимости;

Г) определение слабых мест и недостатков в системе охраны.

 Модель нарушителей определяет:

1. категории (типы) нарушителей, которые могут воздействовать на объект;
2. цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.;
3. типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

Следует учитывать как внешних нарушителей, проникающих на территорию, в зоны, здания и помещения объекта извне, так и внутренних, т.е. из числа штатного персонала объекта или из числа посетителей, имеющих возможность легальным путем получить пропуск либо допуск на объект. Естественно, необходимо учитывать в модели возможность сговора и совместных действий внешних и внутренних нарушителей.

В модель нарушителей следует включать максимально исчерпывающие сведения о действиях нарушителей. Целесообразно также оценивать степени возможности или субъективные вероятности использования нарушителями каждой выделенной категории сценариев и способов действий.

Для объекта необходимо определить все зоны и помещения, при проникновении в которые нарушители могут нанести объекту ущерб определенной категории. Эти зоны, здания и помещения являются целевыми зонами нарушителей. К ним относятся зоны доступа к особо ценным материалам, оборудованию, носителям информации, а также применения огневых или диверсионных средств и проч.

Указанные зоны следует разделить по категориям ущерба. Примерами категорий ущерба являются: неприемлемый ущерб, когда нарушители могут вызвать крупную аварию, похитить особо важные документы, информацию, оборудование; существенный ущерб, когда последствия хищения или диверсии парализуют работу объекта на определенное время; материальный ущерб (большой, средний, малый), когда последствиями будут материальные потери соответствующих масштабов. Категории ущерба упорядочиваются по своей опасности. В целом же категорию зданий и объекта определяет самая опасная категория ущерба особо важных зон в здании и на объекте.

Для каждой категории зоны, здания, объекта следует определить требуемую степень защиты или нормативные показатели уязвимости (эффективности). Показателями уязвимости объекта и его особо важных зон являются степень уязвимости в порядковой шкале оценок (пример степеней: очень высокая, высокая, средняя, ниже средней, низкая) или вероятность успешного воздействия нарушителей в вероятностной шкале. Обратным показателем по отношению к показателю уязвимости является показатель эффективности охраны — степень защищенности объекта (зоны) или вероятность обезвреживания нарушителей до нанесения объекту ущерба.

2. Составление модели угроз

Модель угроз должна быть оформлена в виде законченного документа, имеющего следующую структуру:

Введение
1. Перечень сокращений

2. Перечень нормативных документов

3. Описание объекта информатизации

4. Угрозы безопасности

Заключение.
Приложение А.

Приложение Б.

Приложение В.

**Введение** содержит общие сведения о целях и задачах, а также выбранной методике построения модели безопасности объекта (ФСТЭК, ФСБ, Банка России).

«**Перечень сокращений»** должен содержать все употребляемые в тексте документа сокращения с кратким описанием. Например:

ПК – персональный компьютер

ТС – терминальный сервер

**«Перечень нормативных документов»** содержит нормативно-методические и руководящие документы, в соответствии с которыми осуществлялась работа по построению модели угроз.

Раздел «**Описание объекта информатизации»** является одной из главных частей модели угроз.

Данные должны включать:

* Описание помещений организации и их функциональное назначение.
* Структуру организации.
* используемые технические средства, их назначение. Например:

|  |  |  |
| --- | --- | --- |
| **Идентификатор** | **Описание** | **Примечание** |
| СБД1 | Сервер БД (Активный) | CentOS 6.3 / Ext4 |
| СБД2 | Сервер БД (Резервный) | CentOS 6.3 / Ext4 |
| ТС1 | Терминальный сервер 1 | MS Windows 2008 R2 Enterprise / NTFS |
| ТС2 | Терминальный сервер 2 | MS Windows 2008 R2 Enterprise / NTFS |
| ПК1 | Персональный компьютер 1 | MS Windows 7 Enterprise / NTFS |
| ПК2 | Персональный компьютер 2 | MS Windows 7 Enterprise / NTFS |

Идентификатор служит для быстрого обращения к активу из текста документа, описание служит для понимания, что за техническое средство используется, примечание служит для уточнения данных о технических средствах и их назначениях.

* **детальное описание технических средств.** Как пример: *ТС – терминальный сервер. Подключение удаленных клиентов по протоколу RDP для работы с системой. Подключение происходит с аппаратных тонких клиентов и персональных компьютеров. На терминальном сервере установлено приложение, используемое для работы с базой данных.*
* **Схему подключения технических средств.** *Данная схема должна отражать детальную архитектуру информационной системы.*
* **Реализованные защитные меры.** *Данная информация позволит разработчику модели угроз учесть уже внедренные средства защиты и провести оценку их эффективности, что позвонит с некоторой долей вероятности снизить затраты на закупку средств защиты.*
* **Формирование перечня активов.** *Необходимо определить перечень активов, их значимость для компании и идентификатор для быстрой ссылки из документа.* Например:

|  |  |  |
| --- | --- | --- |
| **Актив** | **Значимость** | **Идентификатор** |
| Коммутационное оборудование | Высокая | КО |
| Внешний канал связи | Высокая | КСвнеш |
| Внутренний канал связи | Высокая | КСвнут |
| Система хранения данных | Высокая | СХД |

В зависимости от выбранной методики оценки рисков, 3 раздел модели угроз может содержать дополнительную информацию. Например, в случае моделирования угроз для персональных данных, данный раздел дополняется «показателями исходной защищенности ИСПДн», «основными характеристиками ИСПДн».

В разделе **«Угрозы безопасности»** описываются результаты моделирования угроз. В описание входит:

* актуальность внешних или внутренних угроз;
* перечень актуальных нарушителей;
* перечень актуальных угроз информационной безопасности.

Перечень актуальных угроз необходимо оформить в виде таблицы:

|  |  |  |
| --- | --- | --- |
| **№** | **Угроза** | **Активы** |
| У-1 | Неавторизованное проникновение нарушителя внутрь КЗ | КО, АРМ, ТК АИБ |
| У-2 | Кража носителей информации, содержащих конфиденциальную информацию | БН, АНИ |
| У-3 | Кража отработанных материалов (мусор, уничтоженные документы, списанные носители) | БН, АНИ |

 При заполнении таблицы можно использовать Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru)

**Заключение** содержит основные выводы и рекомендации по устранению угроз.

 Приложения могут содержать дополнительную информацию. Например, в Приложении А может быть построена модель нарушителя.

 Модель нарушителя включает следующие пункты:

• описания видов нарушителей и их возможностей (внутренние, внешние);

• описание каналов доступа в информационную систему организации (физические, общедоступные, технические)

• описание данных видов нарушителей с привязкой к штатной структуре организации;

• описание возможностей данных нарушителей;

• определение актуальности каждого из видов нарушителей.

 Модель нарушителя может быть оформлена в виде таблицы:

|  |  |  |
| --- | --- | --- |
| **Тип нарушителя** | **Категории нарушителей** | **Идентификатор** |
| Внешний нарушитель | Криминальные структуры, внешние субъекты (физические лица) | N1 |
| Внутренний нарушитель | Лица, имеющие санкционированный доступ в КЗ, но не имеющие доступа к ИСПДн (технический и обслуживающий персонал) | N2 |
| Зарегистрированные пользователи ИСПДн, имеющие доступ к ПДн | N3 |
| Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн | N4 |
| Зарегистрированные пользователи с полномочиями системного администратора ИСПДн | N5 |
| Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн | N6 |

3. Разработка основных положений политики безопасности организации

 На основе анализа уязвимостей и модели угроз участник соревнований должен составить общие положения политики безопасности предприятия или организации.

 Политика безопасности — документ, в котором должны быть указаны:

1. Цели и задачи обеспечения информационной безопасности.

2. Рекомендации по реализации системы защиты.

3. Ответственность персонала.

4. Порядок ввода в действие средств защиты.

5. Порядок пересмотра средств защиты.

6. Политика учетных записей.

7. Политика использования паролей.

8. Политика реализации антивирусной защиты.

9. Меры профилактики нарушений политик безопасности.

10. Ответственность нарушителей политики безопасности

 При работе можно опираться на существующие методики создания политики безопасности и стандарты информационной безопасности (ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL и др.)

**Критерии оценки выполнения конкурсного задания**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Аспект | Балл |
| A1. | Анализ уязвимостей | Подготовительный этап: не оценивается |
| A2. | Модель угроз | Соблюдение структуры документа | 1 |
|  |  | Точность и ясность формулировки цели и задач | 1-3 |
| Обоснованность выбора методики построения модели безопасности | 2-4 |
| Подробность описания объекта информатизации | 1-3 |
| Количество и подробность описания выделенных актуальных угроз | 2-4 |
| Обоснованность выводов и рекомендаций | 2-4 |
| Наличие и содержание Приложений | 2-4 |
| Использование профессиональной терминологии | 1-3 |
| A3. | Разработка основных положений политики безопасности организации | Точность и ясность формулировки цели и задач обеспечения безопасности | 1-3 |
| Соответствие предложенных мер защиты цели и задачам обеспечения безопасности | 2-4 |
| Подробность и обоснованность порядка ввода в действие и порядка пересмотра средств защиты | 2-4 |
| Подробность и обоснованность описания политики учетных записей | 1-3 |
| Подробность и обоснованность описания политики использования паролей | 1-3 |
| Подробность и обоснованность описания политики реализации антивирусной защиты | 1-3 |
| Обоснованность мер профилактики нарушений политики безопасности | 2-4 |
|  | Итого по модулю А | Макс. 50 |

*Второй день.*

**Модуль B - Использование встроенных механизмов разграничения доступа ОС Windows.**

**Модуль C - Использование возможностей ОС Windows по криптографической защите информации.**

*Время выполнения* – 5 часов

Предварительная настройка

Необходимо настроить виртуальную машину Windows Server 2008 используя файл Win2008.vdi

|  |  |
| --- | --- |
| Имя VM | Winsrv2008 |
| Сетевое имя сервера | SrvN. wskills.test |
| Сетевой адрес | 10.1.0.N |
| RAM | 1Gb |
| Количество жестких дисков | 4(Win2008.vdi, и три диска по 1 GB |
| Тип подключения виртуального сетевого | Сетевой мост |
| Подключение к домену wskills.test |  Да  |

Настроить виртуальную машину Windows 7 используя файл Win7.vdi

|  |  |
| --- | --- |
| Имя VM | Win7 |
| Сетевое имя сервера | clnN. wskills.test |
| Сетевой адрес | 10.1.0.1N |
| Количество жестких дисков | 2(Win7.vdi, и диск 1 GB |
| Тип подключения виртуального сетевого | Сетевой мост |
| Подключение к домену wskills.test |  Нет  |

**Модуль B**

Необходимо на сервере SrvN. wskills.test настроить файловое хранилище для хранения отчетов Отдела\_N.

В отделе работают 4 сотрудника: ИвановN ИИ, ПетровN ПП, СидоровN СС, ОрловN ОО

Используя средства управления службой каталогов создать необходимые учетные записи.

Cоздайте файловую структуру вида

D:\Архив\

 Фамилия ИО(1сотр)

….

Фамилия ИО (4сотр)

Итоговые отчеты

Оценка результатов работы

Настроить доступ к папкам таким образом, чтобы пользователи отдела имели возможность:

1. просмотреть данные во всех папках кроме папки Оценка результатов работы.
2. В «своих» папках пользователи должны иметь возможность создать и изменить документы, без возможности удаления документа.
3. В папке Итоговые отчеты пользователи должны иметь возможность только создать, но не изменять документы.
4. В папке Оценка результатов работы создавать, изменять и удалять файлы и каталоги может только Орлов ОО.

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| B1 | Выполнен 1 пункт | 1 |
| B2 | Выполнен 2 пункт | 3 |
| B3 | Выполнен 3 пункт | 3 |
| B4 | Выполнен 4 пункт | 1 |
| B5 | Созданы доменные учетные записи пользователей | 1 |
| B6 | Созданы доменные учетные записи групп, доменные пользователи включены в группу | 2 |
| B7 | Разрешения выдаются с использованием групп | 3 |
| B8 | Используется наследование разрешений | 1 |
| Итого |  | 15 |

Настроить аудит доступа к папке Итоговые отчеты, необходимо фиксировать все неуспешные попытки доступа к отчетам.

Проверить фиксацию попыток удаления и изменения отчетов.

Проверить фиксацию успешных просмотров

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| B9 | Аудит настроен | 2 |
| B10 | Фиксируются неуспешные попытки доступа | 1 |
| B11 | Не фиксируется успешный доступ | 2 |
| Итого |  | 5 |
|  | Итого по модулю B | 20 |

**Модуль С**

Настройте архивацию по расписанию папки с файловым архивом на один из свободных дисков. Архивация должна выполняться каждые полчаса

Настройте ежедневную архивацию по расписанию папки C:\Users в папку D:\Bakups

Проверьте, что резервная копия папки с файловым архивом создана

Восстановите папку итоговые отчеты, в другую папку ( D:\ итоговые отчеты)

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| C1 | Архивирование папки с файловым архивом настроено  | 1 |
| C2 | Архивирование папки C:\Users настроено | 3 |
| C3 | Папка итоговые отчеты восстановлена | 1 |
| Итого |  | 5 |
|  | Итого по модулю C | 5 |

*Третий день.*

**Модуль D - Использование возможностей ОС Windows по обеспечению сохранности информации.**

**Модуль E - Использование USB-токенов (eToken) для повышения защищенности ОС Windows.**

*Время выполнения* – 5 часов

**Модуль D**

На clnN. wskills.test создайте локальные учетные записи для сотрудников отдела

Cоздайте файловую структуру вида

D:\Архив\

 Фамилия ИО(1сотр)

….

Фамилия ИО (4сотр)

Необходимо организовать и реализовать использование встроенных возможностей шифрования для личных папок (Фамилия ИО) в файловом архиве.

Обеспечьте возможность восстановления доступа к данным уволенных сотрудников

Обеспечьте для ИвановN ИИ возможность восстановления доступа к данным после утери ключа шифрования

Необходимо описать порядок восстановления доступа к данным уволенных сотрудников.

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| D1 | Файлы в папках зашифрованы  | 1 |
| D2 | ИвановN ИИ и ПетровN ПП, СидоровN СС и ОрловN ОО могут попарно открывать друг у друга файлы | 1 |
| D3 | Настроен агент восстановления | 2 |
| D4 | Экспортирован сертификат с открытым ключом Иванова  | 1 |
| Итого |  | 5 |

Необходимо на сервере SrvN. wskills.test настроить защищенный доступ по протоколу HTTPS к корневому каталогу.

Необходимо настроить необходимость использования сертификатов пользователями вэб-сервера.

Получить необходимые сертификаты для пользователей виртуальной машины clnN. wskills.test

Все необходимые сертификаты получить с сервера dс. wskills.test используя вэб интерфейс службы сертификатов

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| D5 | Доступ по протоколу HTTPS настроен | 2 |
| D6 | Для доступа необходимо иметь сертификат | 1 |
| D7 | Пользователи clnN. wskills.test могут получить доступ к вэб-серверу | 2 |
| Итого |  | 5 |
|  | Итого по модулю D | 10 |

**Модуль E**

Настроить и проверить использование электронной подписи и шифрование сообщений при обмене электронной почтой.

Для пользователей clnN. wskills.test получить с сервера dс. wskills.test используя вэб интерфейс службы сертификатов и записать на eToken необходимые сертификаты.

Настроить почтовое взаимодействие для пользователей СидоровN СС и ОрловN ОО.

Почтовый клиент Почта Windows Live.

Почтовый сервер dс. wskills.test

Почтовое взаимодействие по протоколу POP3

Оценка данного модуля будет осуществляться по следующим критериям:

|  |  |  |
| --- | --- | --- |
| № | Аспект | Балл |
| E1 | Необходимые сертификаты получены | 2 |
| E2 | Сертификат записан на eToken | 3 |
| E3 | Пользователи настроили почтовое взаимодействие | 3 |
| E4 | Пользователи проверили использование электронной подписи при почтовом взаимодействии | 4 |
| E5 | Пользователи проверили использование шифрование при почтовом взаимодействии | 3 |
|  | Итого по модулю E | 15 |