КОНКУРСНОЕ ЗАДАНИЕ
Финала национального IV межвузовского чемпионата
WorldSkills Russia 2020
по компетенции
«Корпоративная защита от внутренних угроз информационной безопасности»

Модуль. Исследование (аудит) организации с целью защиты от внутренних угроз.

Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз.

- Задания должны быть выполнены в виде отчёта в формате .odt или.doc(x); Графические иллюстрации должны быть внутри документа.
- Итоговый скан документа (с подписью участника) должен быть загружен на рабочий стол RDP сессии под названием ***Модуль_2_Аудит_<Фамилия участника>.расширение***

Участник самостоятельно распечатывает документ, проверяет, расписывается, сканирует и загружает pdf-отчёт на RDP сессию и/или передает сканированный с помощью технического эксперта используя иные каналы связи.
Работа принимается к оценке со сканом копии с подписью конкурсанта для сравнения электронной копии с бумажной на случай расхождений.

Задание. Подготовка аудита информационной безопасности организации

В целях выполнения подготовительных работ для построения Модели угроз информационной безопасности планируется провести аудит информационных систем и процессов организации.

Вам, как специалисту, поручено провести подготовительные мероприятия по подготовке аудита информационной безопасности информационной системы по исходным данным и основываясь на действующих требованиях Российского законодательства по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. В процессе проведения аудита **вы должны решить следующие задачи (задания)**:

1.1 Определить перечень основных объектов информатизации, представленных в организации.

1.1 Определить каналы передачи данных

1.2 Определить перечень субъектов, имеющих доступ к информации, на основании данных Таблицы 1, структура компании и личным опытом работы с AD

1.3 Определить границы доменов доверия (периметр(ы) безопасности).

1.4 Осуществить категорирование (классификацию) представленной в организации информации в соответствие с типами информации ограниченного доступа

Информация	Тип информации ограниченного доступа	Субъекты, имеющие доступ к информации	Комментарии

1.5 Определить перечень актуальных для организации объектов защиты, привести обоснование. Заполнить таблицу.

Объект информатизации	Объект защиты	Обоснование актуальности защиты	Тип объекта защиты согласно определения в ГОСТ Р 50922-2006

1.6 Провести сопоставление типов информации ограниченного доступа ограниченного доступа требованиям законодательства РФ. Идентифицировать перечень нормативно-правовых актов (НПА) РФ и регуляторных документов, требования которых распространяются на организацию (включая Федеральные законы, Постановления правительства, статьи Гражданского и Трудового кодекса, приказы и указания регулятора и т.п.). Заполнить таблицу.

Информация	Тип информации ограниченного доступа	НПА и регуляторные документы

1.7 Составьте перечень основных угроз (рисков) от внутренних утечек информации ограниченного доступа для организации. Приведете пояснения, при необходимости. Рассмотреть только случай, когда источник угрозы безопасности информации (субъект) – внутренний нарушитель, физическое лицо.

1.8 Оценить объём потенциальных финансовых потерь для каждой угрозы (в рублях или долларах). Проведите расчёт угроз (рисков ущерба) при утечке информации ограниченного доступа для разных объектов защиты, дайте необходимые пояснения. Используйте при расчётах методические рекомендации ФСТЭК или профильные ГОСТ, например, «Методику определения угроз безопасности информации в информационных системах». Разрешается использовать альтернативные модели со ссылкой на источник.

1.9 По итогам расчётов оцените приоритеты: составьте перечень угроз в порядке снижения важности для организации, т. е. по снижению уровня потенциальных финансовых потерь.

1.10 В рамках подготовки плана, определить перечень нормативных документов ООО «Демо Лаб», которые необходимо принять для организации мероприятий защиты от внутренних угроз, указанных ранее.

1.11 Во время внутреннего аудита было выявлено, что комплект внутренних нормативных документов не полон. Подготовить шаблон документа «Акт определения уровня …», приведенного вместе с заданием.

1.12 На основе конкурсного задания, подготовьте предложения по усилению контроля циркулирующих в организации (а также

передаваемых за пределы организации) данных с использованием существующей DLP-системы с целью предотвращения утечек информации ограниченного доступа или других инцидентов информационной безопасности.

1.13 Разработайте техническое задание на создание политики для DLP-системы InfoWatch, учитывающую специфику и направление деятельности организации, согласно представленному выше описанию. Политика не должна повторять политики DLP-системы, представленные в любом виде на Чемпионат (качестве конкурсных заданий, DLP-политик «по умолчанию» и т.п.)

Приложение 1. Результаты опроса сотрудников и руководства

Направления работ

Научно-исследовательская компания «Демо Лаб» заказала демоверсию DLP-системы с целью опробовать функциональные возможности программного обеспечения.

Компания «Демо Лаб» занимается (а) контрактной разработкой и (б) продажей перспективных электронных систем в интересах государственных и коммерческих организаций. Также в партнёрстве с компаниями «большой четверка» компания (в) осуществляет аудит сторонних организаций (в части стандартов качества и т. п.), обладая всеми необходимыми для этого лицензиями.

Доходность работ по направлениям

Маржинальность работ, связанных с контрактной разработкой различного рода систем (НИР/НИОКР) составляет 20%, от продаж электронной компонентной базы (собственной и сторонней разработки) – 50%, от аудиторской деятельности – 50%.

Средняя стоимость контракта на разработку – 100 млн рублей (всего за 1 контракт), средний период исполнения - 2 года. В год заключается, в среднем, 20 контрактов. Тематики работ носят несекретный, но закрытый характер, например: разработка перспективных систем космической связи, радиолокационных станций, систем связи, систем автоматизации для органов государственной власти и т. п.

Средняя стоимость договора поставки электронных компонент – 20 000 долларов, длительность поставки – 2 недели. В год 2000 «средних продаж».

Договора по участию в аудиторской деятельности приносят 1 млн. $ в год.

Также у компании есть договор с государственными органами об организации государственных закупок по отдельным категориям продуктов

путём организации торгов (т. е. компания действует как оператор торгов). В рамках организации торгов компания занимается сбором заявок, предоставляемых участниками торгов в соответствии с правилами организованных торгов в соответствии с требованиями 325-ФЗ. Данная деятельность убыточна для организации, но положительно сказывается на её репутации.

Сведения ограниченного характера и потенциальные потери

Компания обладает интеллектуальной собственностью (охраняемой в режиме «ноу хау», охрана секретов производства). Это, преимущественно - результаты НИР и НИОКР, проектно-технологическая документация. Сохранение в тайне этих данных крайне важно, т. к. именно они обеспечивают техническое превосходство над конкурентами, составляя основу создаваемых и реализуемых технических решений. По статистике в компаниях аналогичного типа утечки подобного рода происходят 1 раз в 4 года.

«Соглашение о конфиденциальности», которые компания заключает с заказчиками НИР/НИОКР, содержит пункт о фиксированном штрафе в 20 млн рублей за подтверждённую утечку данных в рамках текущего контракта.

Компания реализует проекты как самостоятельно, так и использует механизм субподряда, нанимая сторонние организации для разработки части модулей/систем, а также взаимодействуя с академическими партнёрами (преимущественно, государственные КБ, ВУЗы, НИИ). При этом в рамках договорных отношений компания может получать конфиденциальную информацию от контрагентов.

Компания обладает значительной клиентской базой, детальной информацией о партнёрах, заказчиках, клиентах за 10 лет работы. Клиентская база составляет основу для деятельности по направлению продаж электронных компонент, но не оказывает влияния на направление системных разработок. Потеря базы клиентов и её использование конкурентами (например, в результате кражи базы инсайдерами) может привести к потере 50% продаж в текущем и 20% следующем году. В целом по отраслевой статистике кража базы или

переход менеджера с базой продаж на работку к конкурентам происходит 1 раз в 4 года.

Разглашение закрытых сведений, связанных с ноу хау и новыми техническими решениями компании при контрактной разработке ставит под вопрос репутацию компании, её способность адекватно проводить работы в интересах гос. компаний. Это может серьезно повлиять на продажи и перспективные контракты. Ухудшение репутации приводит к потере 5% ключевых заказчиков на разработку системных решений в течение 5 лет и потери 20% продаж в течение 3 лет. Участие в аудиторской деятельности становится невозможно в долгосрочной перспективе.

Основой для документооборота компании и организации бизнес-процессов является ERP Microsoft Dynamics. Остановка его работы на срок более 1 суток приводит к полной остановке деятельности по направлениям аудит и продажи (потери прямо пропорциональны (линейно) от времени неработоспособности данного ПО).

С точки зрения кадрового, бухгалтерского и финансового документооборота компания является типовой для Российской федерации.

Сотрудники могут обмениваться информацией посредством Почты/Email, мессенджеров/WhatsApp. Также у ряда сотрудников есть корпоративные сотовые телефоны, через которые также проходит обмен информацией.

Вы — администратор безопасности организации, ответственный за обеспечение защиты компании от внутренних угроз.

Ваша задача провести анализ циркулирующей в копании информации, определить перечень внешних нормативно-правовых актов, регулирующих использование информации ограниченного доступа в организации, а также подготовить соответствующие документы и внутреннюю нормативную базу для законного применения средств защиты информации.

Ваша итоговая цель — провести анализ компании, выявить объекты защиты, определить нормативно-правовую базу для принятия мер по защите информации, разработать непротиворечивый план мероприятий по усилению защиты организации от угроз информационной безопасности, а также составить планы по подготовке

соответствующей внутренней нормативной базы.

Допущение 1: предполагается, что дополнительные документы в компании, касающиеся информационной безопасности и документооборота (положения, приказы и т. п.) могут и должны быть обновлены в соответствии с результатом аудита, разрабатываемым набором документов по ИБ моделью угроз ИБ и не влияют на итоговый результат.

Допущение 2: предполагается, что весь перечень нормативных и технических работ, связанных с защитой гос. тайны уже выполнен. В компании недавно была проверка регулятора по защите гос. тайны, все требования регулятора выполнены

Допущение 3: на основании предыдущего опыта компании и в результате анализа деятельности аналогичных организаций все угрозы утечек информации ограниченного доступа равновероятны, вероятность (возможность) реализации каждой угрозы равна $\mathbf{P_j=0.05}$.

ИСХОДНЫЕ ДАННЫЕ

Примечание: Сформулированные исходные данные организации в точности соответствуют базе данных организации, расположенной на сервере AD.

Структура компании

Группа ТМ	Кол-во сотрудников	Информационные системы	Циркулирующие данные
Бухгалтерия (Accounting)	8	1С Бухгалтерия	Финансовая и бухгалтерская информация
Отдел договоров (Financial)	10	1С Предприятие/ Бухгалтерия, СУБД,	Финансовая информация, тендерная документация, договора
Совет директоров (BOD)	3	Управленческие отчёты, 1С Предприятие в части подготовки отчётов	Весь объём информации
Отдел кадров (HR)	3	1С Предприятие, СУБД,	Документы кадрового документооборота
Информационные технологии (IT)	10	SVN, трекеры проектов, средства разработки (VS, Matlab, LabView др.) СУБД, в т. ч. база проектно-технологической документации САПР Облачное моделирующее ПО	Информация НИР/НИОКР, информация аудита внешних компаний, ноу-хау
Отдел продаж (Sales)	15	СУБД, База данных клиентов	База электронных компонент и продаж
Тендерный	7	Тендерное ПО сторонних	Тендерная

комитет (Tenders)		организаций, системы ЭЦП	информация

Таблица 1

В AD компании для каждого сотрудника указаны следующие атрибуты:

1. Фотография
2. Фамилия
3. Имя
4. Должность
5. Отдел
6. Электронная почта
7. Мобильный телефон
8. Skype/WhatsApp