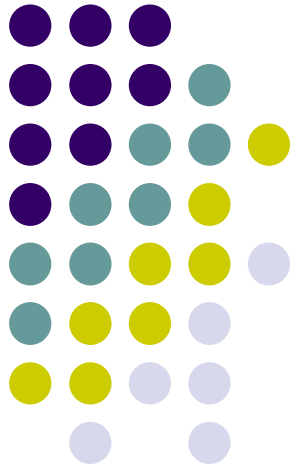
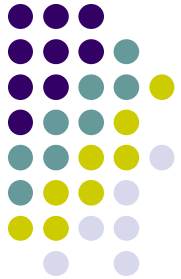
Auditul securității informaționale

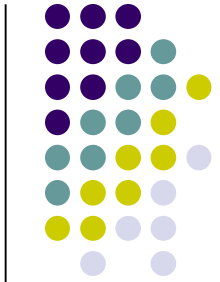
Auditul IT



Agenda

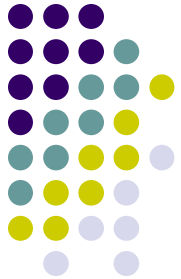


1. Resursele auditate
2. Tipuri și modele de amenințări
3. Activitățile auditorului IT
4. Proceduri și mecanisme de control al auditului intern



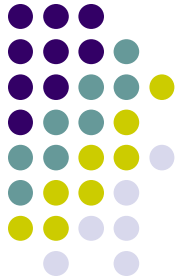
Resursele auditate

Категории ресурсов



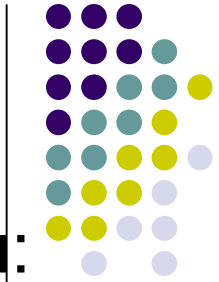
- Информационные ресурсы;
- Программное обеспечение;
- Технические средства (серверы, рабочие станции, активное сетевое оборудование и т. п.);
- Людские ресурсы;
- Финансовые ресурсы.

Основные вопросы обследования безопасности



- Как устроена система? (описание системы)
- Что, от чего и от кого нужно защищать? (модель ресурсов, модель угроз, модель злоумышленника)
- Как это нужно защищать? (выбор контрмер)
- Оценка возможного ущерба и стоимости реализации контрмер (управление рисками)
- Выбор адекватных контрмер

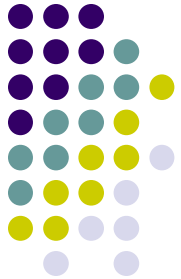
Исходные данные аудита



Аудитору требуется следующая документация:

- Схема организационной структуры пользователей;
- Схема организационной структуры обслуживающих подразделений
- Функциональные схемы;
- Описание автоматизированных функций;
- Описание основных технических решений;
- Другая проектная и рабочая документация на информационную систему

Модель ресурсов

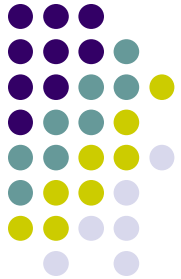


- Физическое размещение серверов, рабочих станций и сетевого оборудования на площадках и в офисах
- Размещение информационных и программных ресурсов на серверах и рабочих станциях
- Приложения, работающие с информационными ресурсами
- Обслуживающий персонал, отвечающий за функционирование приложений и оборудования
- Взаимосвязи между бизнес-задачами, приложениями, данными и оборудованием

Определение ценности ресурса

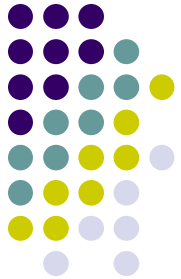
Ценность ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса. Обычно рассматриваются следующие виды ущерба:

- Данные были раскрыты, изменены, удалены или стали недоступны;
- Аппаратура была повреждена или разрушена;
- Нарушена целостность программного обеспечения.



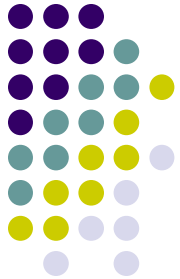
Tipuri și modele de amenințări

Понятие угрозы безопасности



- Источник
- Способ осуществления
- Используемые уязвимости защиты
- Объект нападения

Модель угроз



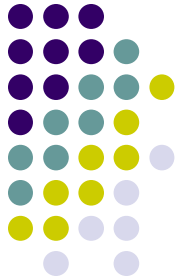
Категории угроз:

- угрозы доступности;
- угрозы целостности;
- угрозы конфиденциальности.

Группы угроз:

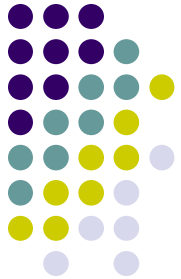
- Угрозы, реализуемые с использованием технических средств;
- Угрозы, реализуемые с использованием программных средств;
- Угрозы, реализуемые путем использования технических каналов утечки информации.

Категории угроз безопасности

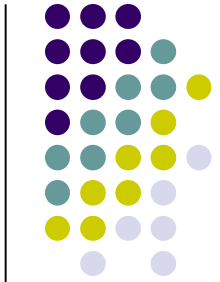


- Локальные и удаленные атаки на ресурсы ИТ\ИС;
- Стихийные бедствия;
- Ошибки, либо умышленные действия персонала ИТ\ИС;
- Сбои в работе ИТ\ИС, вызванные ошибками в программном обеспечении или неисправностями аппаратуры.

Модель нарушителя

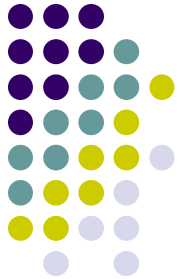


- Определение понятия *нарушителя* и *нарушения* безопасности
- Категорирование нарушителей
- Предположения о квалификации и возможностях каждой категории нарушителей
- Уровень полномочий и способы получения доступа к ИС для каждой категории нарушителей



Activitățile auditorului IT

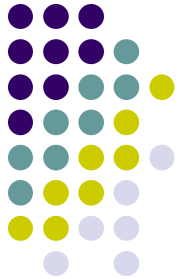
Вопросы аудитора IT



Обычно, в ходе интервью аудитор задает опрашиваемым следующие вопросы:

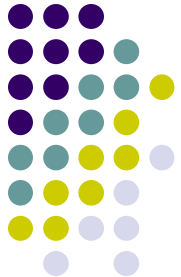
- Кто является владельцем информации?
- Кто является пользователем (потребителем) информации?
- Кто является провайдером услуг?
- Какие услуги и каким образом предоставляются конечным пользователям?
- Какие основные виды приложений, функционирует в ИС?
- Количество и виды пользователей, использующих эти приложения?

Вопросы аудитора (продолжение)



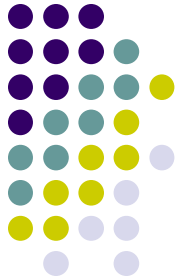
- Из каких компонентов (подсистем) состоит ИС?
- Функциональность отдельных компонент?
- Где проходят границы системы?
- Какие точки входа имеются?
- Как ИС взаимодействует с другими системами?
- Какие каналы связи используются для взаимодействия с другими ИС?
- Какие каналы связи используются для взаимодействия между компонентами системы?
- По каким протоколам осуществляется взаимодействие?
- Какие программно-технические платформы используются при построении системы?

Анализ данных аудита (оценка рисков)



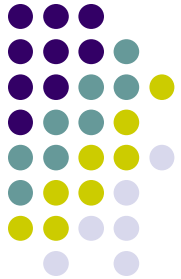
- Анализ ресурсов ИС
- Анализ групп задач, решаемых системой, и бизнес процессов
- Построение (неформальной) модели ресурсов ИС
- Оценка критичности информационных ресурсов, а также программных и технических средств
- Определение критичности ресурсов с учетом их взаимозависимостей
- Определение наиболее вероятных угроз безопасности и уязвимостей защиты
- Оценка вероятности осуществления угроз, величины уязвимостей и ущерба
- Определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость

Оценка соответствия требованиям стандартов



- Аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой ИС и ее соответствие этим требованиям.
- Данные о соответствии различных областей функционирования ИС требованиям стандарта, обычно, представляются в табличной форме.
- Из таблицы видно, какие требования безопасности в системе не реализованы.
- Исходя из этого, делаются выводы о соответствии обследуемой ИС требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие.

Выработка рекомендаций по результатам аудита



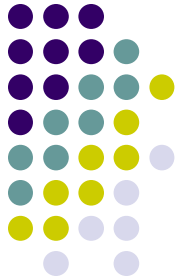
Рекомендации аудитора должны быть:

- конкретными и применимыми к данной ИС,
- экономически обоснованными,
- аргументированными (результатами анализа) и
- отсортированными по степени важности.

При этом:

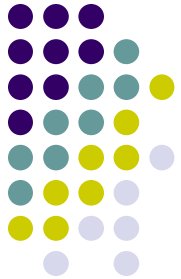
- мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет
- над конкретными программно-техническими методами защиты.

Подготовка отчетных документов по результатам аудита



Аудиторский отчет должен содержать:

- Описание целей проведения аудита,
- Характеристику обследуемой ИС,
- Указание границ проведения аудита и используемых методов,
- Результаты анализа данных аудита,
- Выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие ее требованиям стандартов,
- Рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

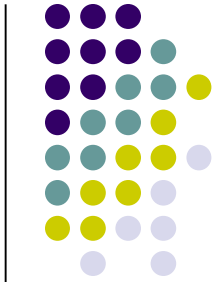


Proceduri și mecanisme de control al auditului intern IS/IT

Цели контроля информационной безопасности

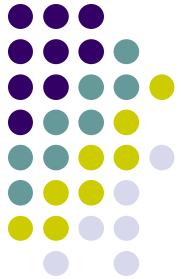
- Защита от вирусов
- Фильтрация спама
- Обеспечение конфиденциальности переписки
- Обеспечение высокой доступности информационных сервисов
- Своевременная установка критичных обновлений ПО
- Защита от несанкционированного доступа к информации
- Обеспечение целостности критичных файлов и баз данных
- Защита от мошенничества в электронных платежных системах

Механизмы контроля



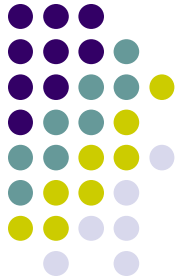
- Превентивные
- Детектирующие
- Корректирующие

Превентивные механизмы контроля



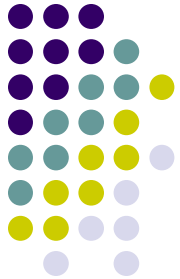
- Упреждающее выявление и предотвращение проблемных ситуаций
- Создание барьеров на пути реализации угроз
- Резервирование
- Разделение ролей
- Использование средств разграничения доступа
- Контроль доступа в помещения
- ....

Детектирующие механизмы контроля



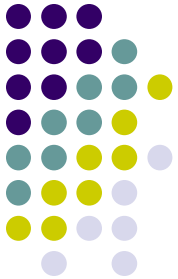
- Выявление проблемных ситуаций и нарушений безопасности во время или после их появления
- Мониторинг событий безопасности
- Обнаружение сетевых атак
- Антивирусное сканирование
- Проверка контрольных сумм файлов
- Процедуры внутреннего аудита
- ...

Корректирующие механизмы контроля



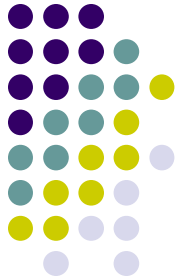
- Разрешение проблемных ситуаций, выявленных при помощи детекритующих механизмов контроля
- Реагирование на нарушения безопасности
- Ликвидация последствий осуществления угроз и минимизация ущерба
- План восстановления после аварии
- Резервное копирование и восстановление данных
- ...

Примеры контрольных процедур



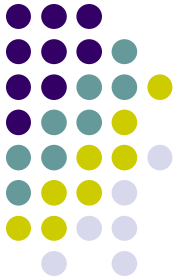
- Разработка и реализация стратегии, политик, стандартов и процедур обеспечения ИБ
- Мониторинг безопасности
- Предоставление доступа к ресурсам корпоративной сети
- Администрирование БД, почтовых серверов и т.п.
- Сетевое администрирование
- Внесение изменений в ПО
- …

Контрольные процедуры внутреннего аудита



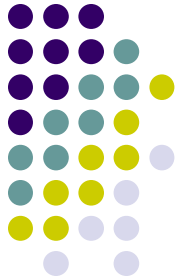
- Ежедневный мониторинг событий безопасности и выявление нарушений
- Еженедельный мониторинг безопасности
- Ежеквартальный (промежуточный) аудит
- Ежегодный комплексный аудит

Ежедневный мониторинг событий безопасности



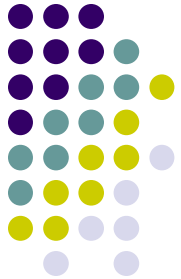
- Изменение сетевых политик безопасности
- Получение доступа к сетевым ресурсам
- Изменение полномочий и учетных записей пользователей и групп
- Сетевые атаки и попытки сканирования
- Изменение конфигурации телекоммуникационного оборудования
- Запуск/останов критичных сетевых сервисов
- ....

Еженедельный мониторинг безопасности



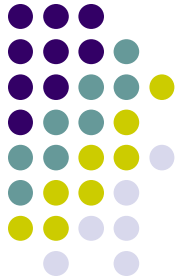
- Контроль состава сетевых административных групп
- Контроль процедуры предоставления доступа к информационным ресурсам
- Контроль прохождения процедуры резервного копирования
- Контроль состояния системы антивирусной защиты и фильтрации спама
- Контроль прохождения процедуры установки критичных обновлений ПО
- ...

Ежегодный комплексный аудит безопасности



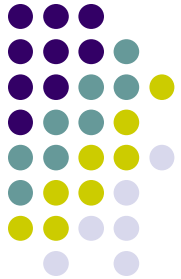
- Проверка реализации парольной политики и учетных записей
- Проверка реализации политики управления доступом
- Проверка реализации политики взаимодействия с сетью Интернет
- Проверка реализации политики удаленного доступа
- Проверка реализации политики обеспечения безопасности платежных систем
- Проверка реализации антивирусной политики
- Проверка системы резервного копирования и восстановления данных
- Проверка выполнения требований политики обновления ПО
- Проверка выполнения инструкций по обращению с информацией ограниченного распространения
- ...

Проверка реализации парольной политики и учетных записей



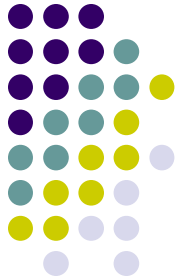
- Проверка настройки параметров парольной политики
- Проверка учетных записей, у которых пароль не менялся более 180 дней
- Проверка заблокированных учетных записей
- Проверка состава административных групп
- Проверка состояния учетных записей и почтовых ящиков уволенных сотрудников
- Внесение корректировок в парольную политику по результатам аудита

Проверка реализации политики взаимодействия с сетью Интернет



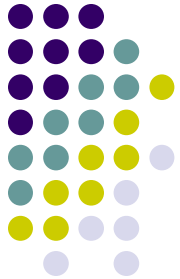
- Проверка списков контроля доступа МЭ (разрешенные протоколы, порты и IP-адреса)
- Проверка выполнения требований по защите каналов взаимодействия с сетью Интернет
- Проверка состава и уровня защищенности хостов, расположенных в DMZ
- Проверка защищенности внешнего периметра корпоративной сети
- Внесение корректировок в политику взаимодействия с сетью Интернет по результатам аудита

Проверка реализации политики резервного копирования



- Проверка наличия, соблюдения и актуальности регламента резервного копирования
- Проверка наличия и актуальности инструкций по выполнению резервного копирования и восстановления данных
- Проверка наличия и правильности ведения журналов резервного копирования
- Проведение тестового восстановления данных с резервных копий на сервере восстановления
- Проверка конфигурации системы резервного копирования
- Проверка режима хранения (и транспортировки) резервных копий
- Внесение корректировок в политику резервного копирования по результатам аудита

Ссылки на Web-ресурсы



- Информационный портал ISO27000.ru: http://www.iso27000.ru
- Интернет-магазин GlobalTrust.ru: http://www.gtrust.ru
- Корпоративный сайт GlobalTrust: http://www.globaltrust.ru

Q&A?

Întrebările, sugestiile, propunerile Dvs. contează pentru toți!!!

Vă mulțumesc!