سیستم های اطلاعاتی حسابداری

نویسندگان:

دکتر مهدی مرادی

(دانشیار دانشگاه فردوسی مشهد)

نعیمه بیات

بسم الله الرحمن الرحیم

فصل هفتم:

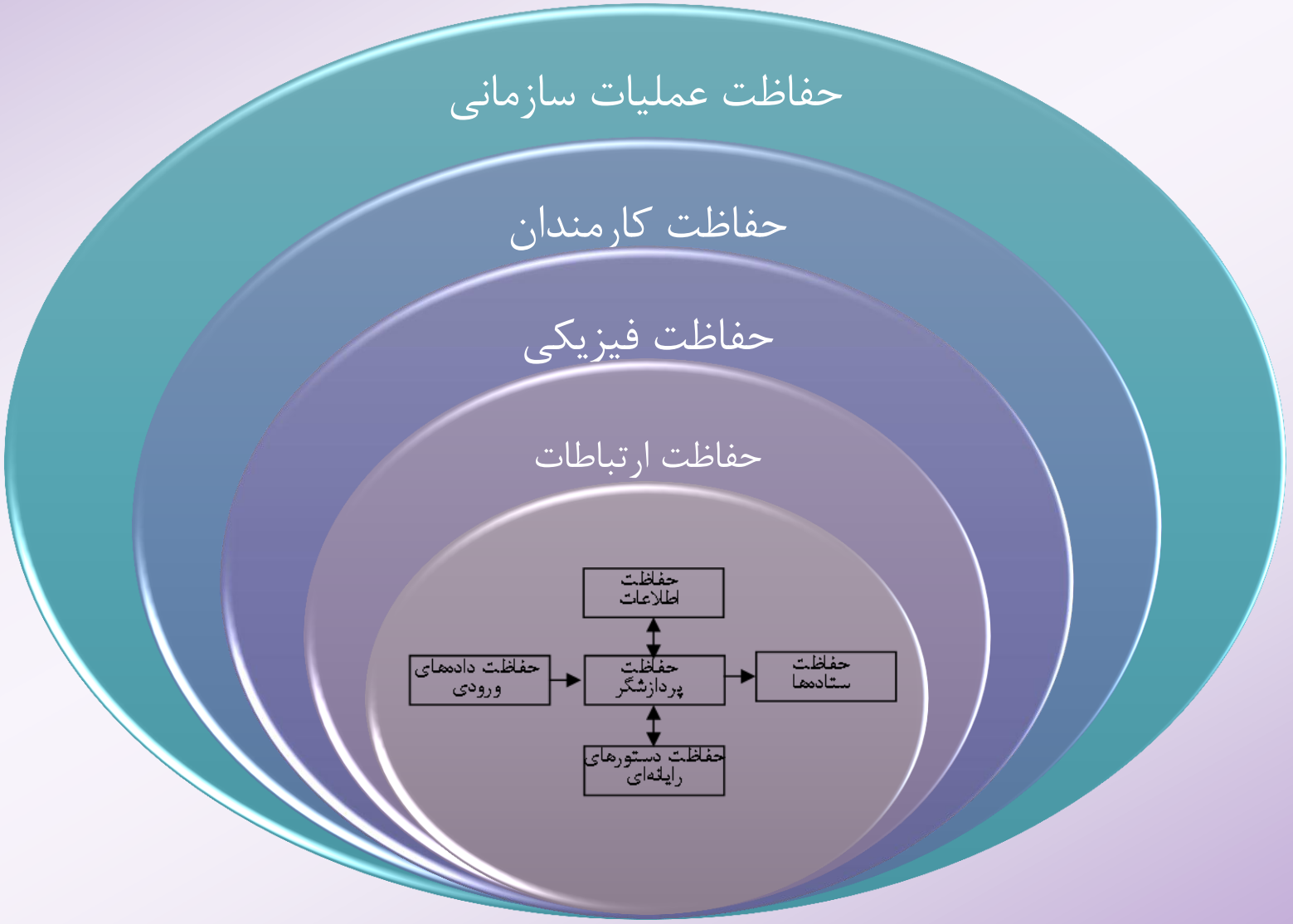
تکنیک های سوء استفاده و تقلب رایانه ای

پس از مطالعه این فصل، خواننده با مفاهیم ذیل آشنا می شود:

۱. آشنایی با انواع تکنیک‌های سوء استفاده و تقلب رایانه‌ای
۲. آشنایی با انواع تکنیک‌های مهندسی اجتماعی
۳. آشنایی با تفاوت میان برخی از روش‌های تقلب
۴. آشنایی با آمار انواع تقلب ها و جرایم رایانه‌ای

اطلاعات یکی از ارزشمندترین دارایی های هر سازمانی است و لذا به کارگیری روش های مطمئن برای حفاظت از اطلاعات ضرورتی انکارناپذیر است :

لایه های حفاظتی سیستم های اطلاعاتی رایانه ای



شکست های لایه حفاظتی داده ها و ارتباطات

تهدیدهای داده ها

- نشت اطلاعاتی
- تحلیل پیام‌های مبادله شده

تهدیدهای نرم افزاری

- مسیرهای میان بُر
- راهزنی نوبت کاربر
- تهدیدهای ناشی از زمان بندی
- اسب تروا
- ویروس‌های رایانه ای
- کرم رایانه ای
- تهدید سالامی
- بمب سیستمی
- حمله سرکاری
- هک کردن
- هجونامه (اسپم)
- اسپوفینگ

شکست های لایه حفاظت فیزیکی

- دور ریختن زباله
- استراق سمع تلفنی
- استراق سمع به شیوه دریافت امواج
- توقف یا تاخیر در سرویس دهی

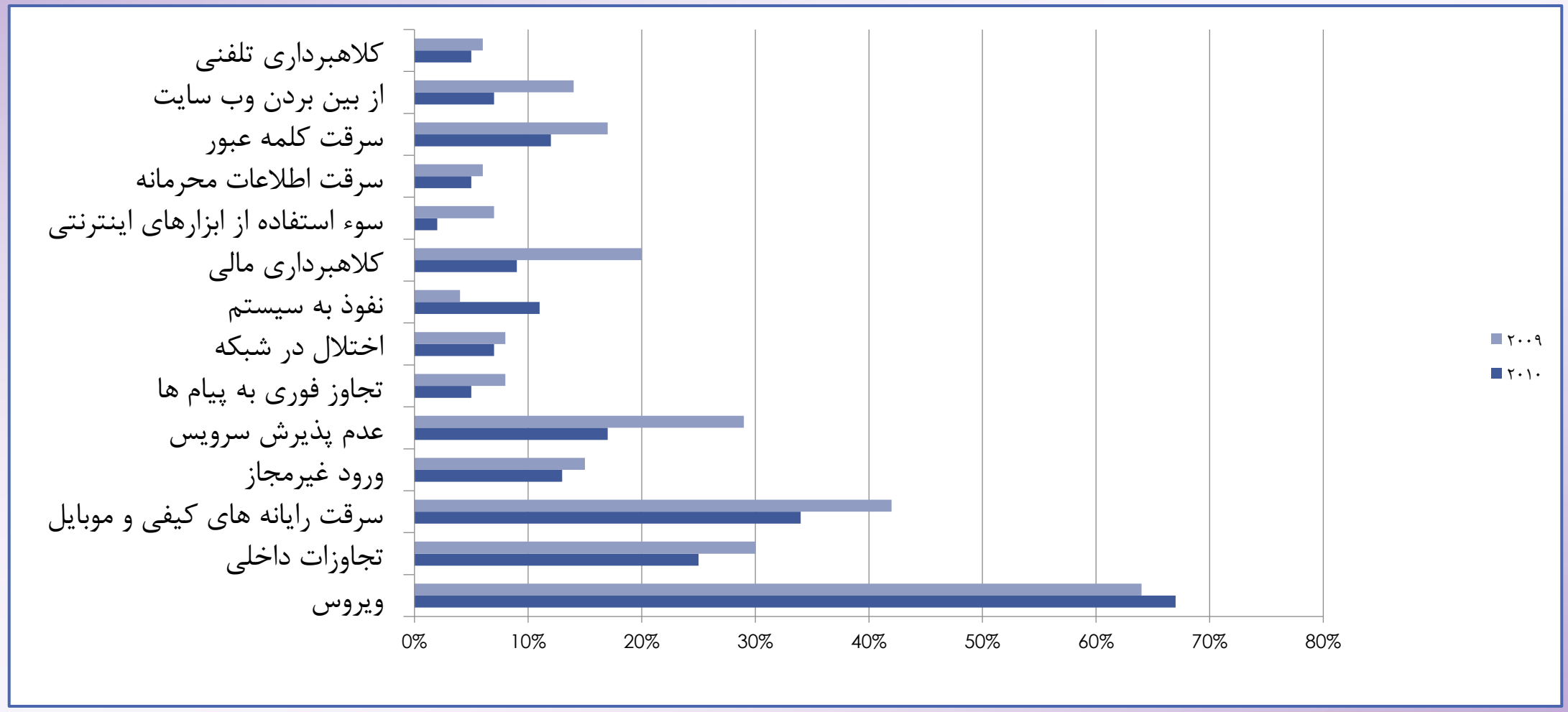
شکست های لایه حفاظت از افراد درون سازمانی

- جعل هویت
- کولی گرفتن
- مهندسی اجتماعی
- سرقت هویت (فیشینگ)
- فارمینگ
- مزاحمت
- نسخه‌برداری غیرمجاز از نرم‌افزار

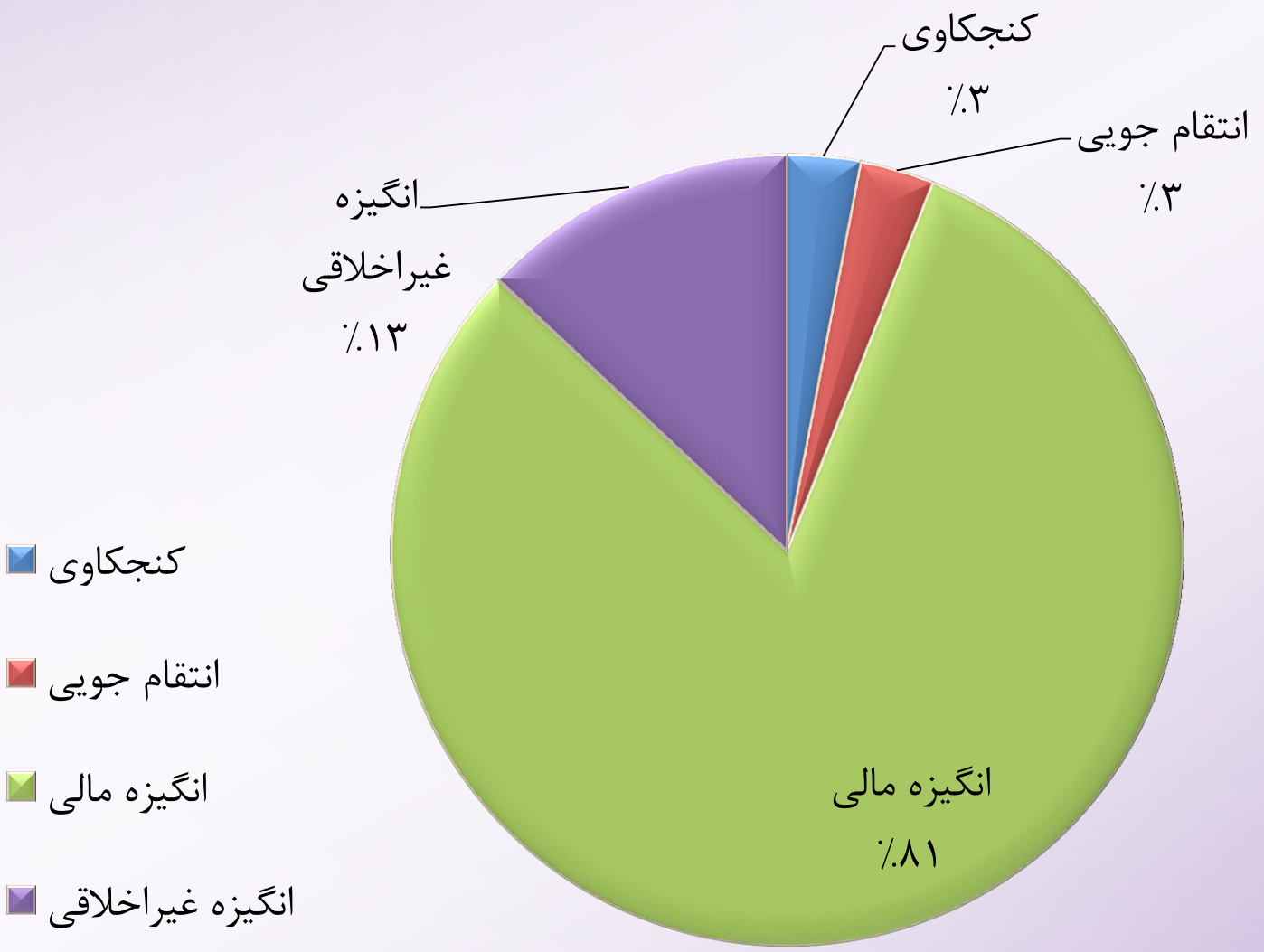
شکست های لایه حفاظت از عملیات

- شکستن کلمه عبور
- جستجوی تلفنی
- کراس سایت اسکریپ تینگ
- اختیارات نامحدود

انواع تقلب‌های رخ داده در سال های ۲۰۱۰و ۲۰۰۹



درصد هریک از انواع جرایم رایانه ای در ایران




اللهم صل علی محمد و آل محمد