



Банк высокой культуры

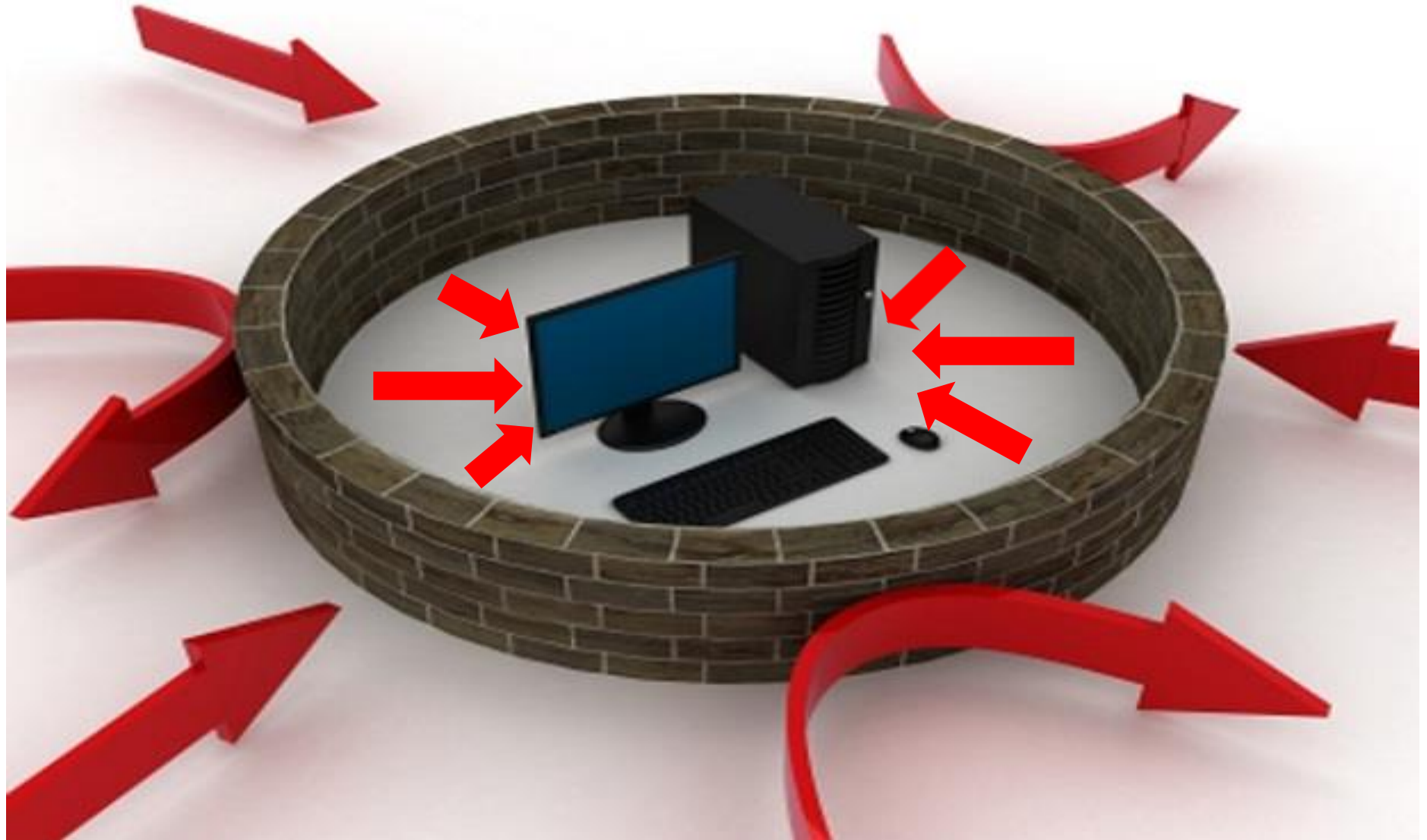
Как бороться с инсайдерами?

Скородумов Анатолий Валентинович

Заместитель директора –

Начальник управления по обеспечению информационной безопасности

Внешние и внутренние угрозы



Кто такой инсайдер?



Предпосылки к появлению внутренних мошенничеств

- Избыточные права доступа
- Отсутствие необходимого контроля
- Отсутствие четко определенных функций подразделений и отдельных работников
- Ошибки при реализации бизнес или технологические процессов
- Нездоровая атмосфера внутри коллектива
- Отсутствие внутрикорпоративной политики по предупреждению внутренних злоупотреблений

Основные методы защиты от инсайда

- Знай своего сотрудника
- Учет мест хранения и способов обработки критичной информации
- Контроль каналов получения и распространения критичной информации
- Реализация процедур по выявлению и пресечению известных схем мошенничества
- Оценка возможных рисков при внедрении новых технологий, продуктов и услуг
- Повышение осведомленности работников в вопросах ИБ

Системы защиты от деятельности инсайдеров

- Использование системы защиты от утечки (DLP)
- Мониторинг запросов пользователей к БД
- Мониторинг обращений пользователей к общим каталогам
- Использование систем фрод-анализа для выявления внутренних мошенников
- Использование систем управления правами доступа
- Использование систем контроля за работой привилегированных пользователей

Средства выявления аномалий как элемент выявлений внутренних злоупотреблений

- Аномалии в запросах пользователя в АС
- Аномалии сетевой активности
- Аномалии в работе с приложениями
- Аномалии при работе с файлами, с устройствами внешнего хранения данных
- Аномалии в выполнении бизнес задач



Инсайд – это не преступление?

«Многие так поступают или поступили бы на моём месте»

«Я не знал, что этого делать нельзя»

«Я заслуживаю этого, мой вклад в организацию больше того, что я получаю в виде зарплаты»

«Я никому ничего плохого не сделал»

«Организация сама виновата в том, что не заботится о своей собственности»

«Я - честный человек, если бы я не был настолько честен, то я мог бы взять намного больше»

Неотвратимость наказания



Fishki.net

ГЛАВНОЕ НЕ ТЯЖЕСТЬ НАКАЗАНИЯ
а его неотвратимость...



Банк высокой культуры

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@mail.ru

Телефон (812) 329-50-64

Благодарю за внимание!