ГАЗПРОМБАНК
В МАСШТАБАХ СТРАНЫ, В ИНТЕРЕСАХ КАЖДОГО

25 лет

Как вычислить инсайдеров в банке?

Москва,
апрель, 2015

Классификация инсайдеров

По характеру целевой информации

- Сбор информации о клиентах (БТ)
- Сбор информации о технологических процессах (КТ)
- Сбор информации о безопасности и защите материальных ценностей, электронных денег.

Классификация инсайдеров

По типу хищения:

- Хищение средств **банка** (ценностей, денег), в т.ч. электронных
- Хищение средств (ценностей, денег) **клиентов**, в т.ч. электронных
- Хищение мат. ценностей (оборудования) банка (безотносительно информации на нем)

Классификация инсайдеров

По цели воздействия:

- Использование должностного положения для помощи третьим лицам в получении услуг банка или сокрытия нарушений клиента
- Использование ресурсов банка для личного обогащения, второй-третьей работы и пр.

Режим информационной безопасности

1. Классификация информации
2. Классификация допусков пользователей
3. Построение перечня каналов доступа и передачи информации, определение персонализированных мест хранения (АБС, порты ввода-вывода, съемные носители, несъемные носители, почта, сетевой трафик).
4. Средство автоматизации, осуществляющее поиск информации в каналах доступа и передачи информации, персонализированных местах хранения, классификацию информации, сравнение информации с допусками.

Выявление «несунов», импортный алгоритм

1. Несовпадение при проверке биографических данных;
2. Кандидат жалуется, что предыдущие работодатели … …. ему не доверяли;
3. Сотрудник знает того, чего знать не должен знать по уровню допуска;
4. Сотрудник хвалится, что может обойти действующую систему защиты;
5. Завидя начальника, сотрудник быстро переключает экран монитора;
6. Сотрудник редко ходит в отпуск;
7. Сотрудник негативно реагирует на изменение своего положения в компании.

Типовые технические способы выявления инсайдеров

1. Наличие информации, не соответствующей должностным обязанностям
2. «Нестандартная» активность
3. Активное «заметание» следов
4. Применение стандартных правил корреляции событий («защита от дурака»).

Типовые организационные способы выявления инсайдеров

1. Нелогичное или частично логичное объяснение своих действий
2. Неудовлетворенность работой
3. Хвастовство перед коллегами или подозрения со стороны коллег, руководителя, значительные переработки по часам (излишняя преданность работе).
4. Что сотрудник принес с собой когда пришел к нам на работу?
5. Связаться с коллегами по ИБ с прежнего места работы.

ДОКЛАДЧИК

Плешков Алексей Константинович

начальник Управления

режима информационной безопасности

Департамента защиты информации
Банка ГПБ (АО) г. Москва

e-mail: Alexey.Pleshkov@gazprombank.ru
тел: 8(495)-428-5045