Самарский государственный университет
Механико – математический факультет

Кафедра безопасности информационных систем
Специальность «Организация и технология защиты информации»

Разработка рекомендаций по работе с персоналом для обеспечения информационной безопасности организации

Дипломная работа

Выполнил студент
Курса 5 группы 20501.10
Малахов Ярослав Владимирович

Научный руководитель
ст.преподаватель
Волков Антон Александрович

Самара 2014г.

Актуальность

Актуальность данной работы состоит в том, что большинство угроз информационной безопасности так или иначе связано с человеческим фактором.

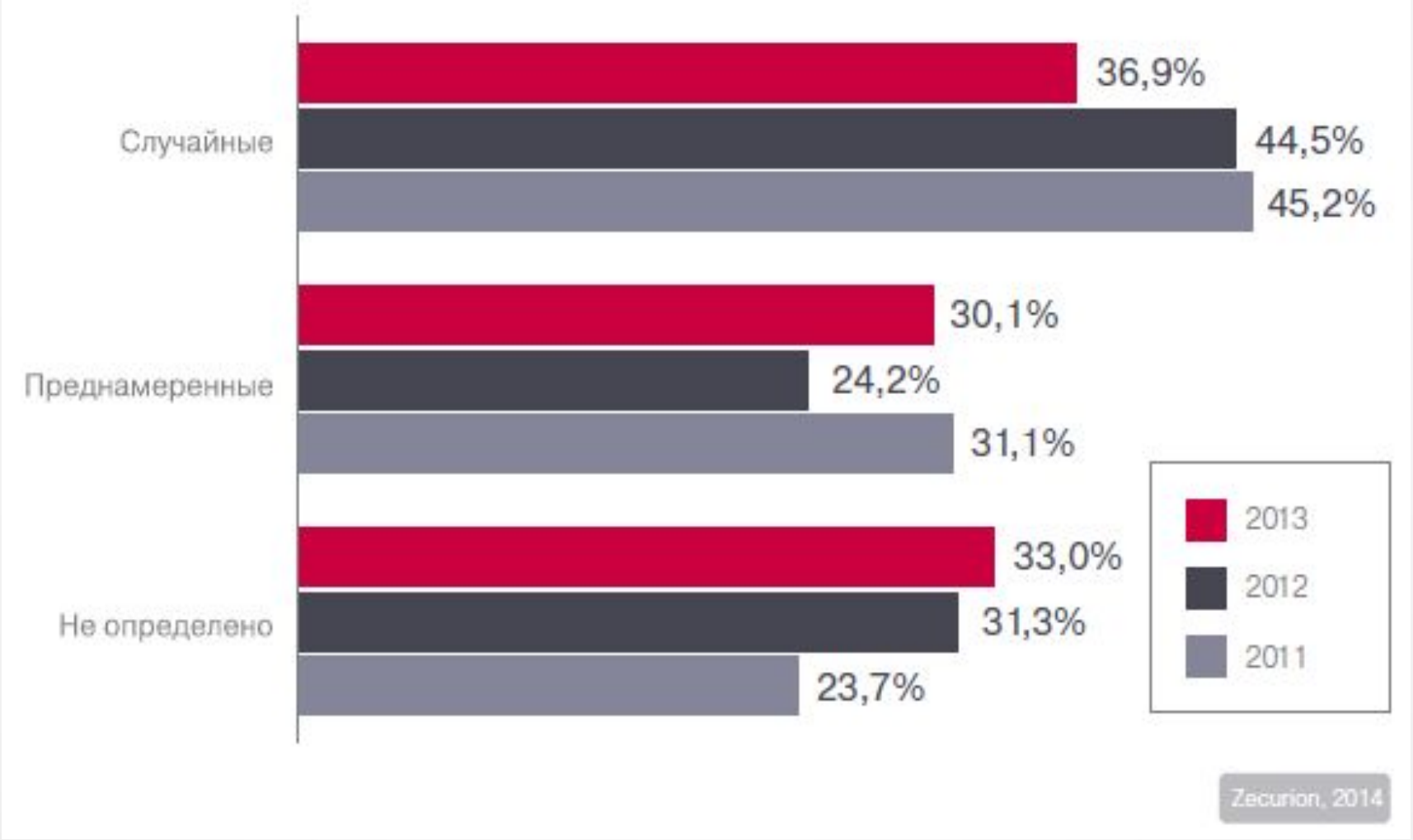
Цель и задачи

Целью данной дипломной работы является разработка рекомендаций по работе с персоналом для обеспечения информационной безопасности организаций. Достижение этой цели достигается путем выполнения следующих задач:

- выявление известных уязвимостей человека, как носителя информации;
- разработка или дополнение новых правил приёма на работу;
- реорганизация или реформация порядка проведения испытательного срока;
- разработка поправок в проведение контроля рабочего процесса сотрудников.

Характер утечки информации

Преобладающая доля утечки информации (36,9%) является следствием человеческих ошибок или халатности, но не являются преднамеренными.



Человеческий фактор как угроза информационной безопасности

Уязвимости	Первопричины
Подкуп	Алчность, жажда «легких денег»
Шантаж	Боязнь краха репутации и потери положения в социуме
Насилие	Инстинкт самосохранения
Психотропное воздействие	Отсутствие возможности мгновенно и самостоятельно выводить вредные вещества из организма
Психотронное воздействие	Отсутствие естественной защиты от излучений
Дезинформация	Из-за неточности информации велик риск получения ложных сведений, которые впоследствии могут привести к негативным последствиям, как для отдельных людей, так и для организации в целом.

Меры пресечения уязвимостей

Распространенными способами устранения уязвимостей в виду возможности законного воздействия являются следующие:

- Корпоративная пропаганда
- Повышение мотивации сотрудника
- Применение санкций (в случае нарушений)

Этапы работы с персоналом

Этап	Цель
Подбор персонала	Выявление уязвимых кандидатов и внедряющихся агентов
Испытательный срок	Тестирование для поиска ранее не замеченных уязвимостей
Работа с постоянным персоналом	Подавление возможности возникновения утечки информации через сотрудников
Увольнение	Сведение возможных последствий к минимуму

Модели собеседований

- Стресс – собеседование:

  “Перекрестный опрос”

- Американский метод собеседования

  Наблюдение за кандидатами в неформальной обстановке.

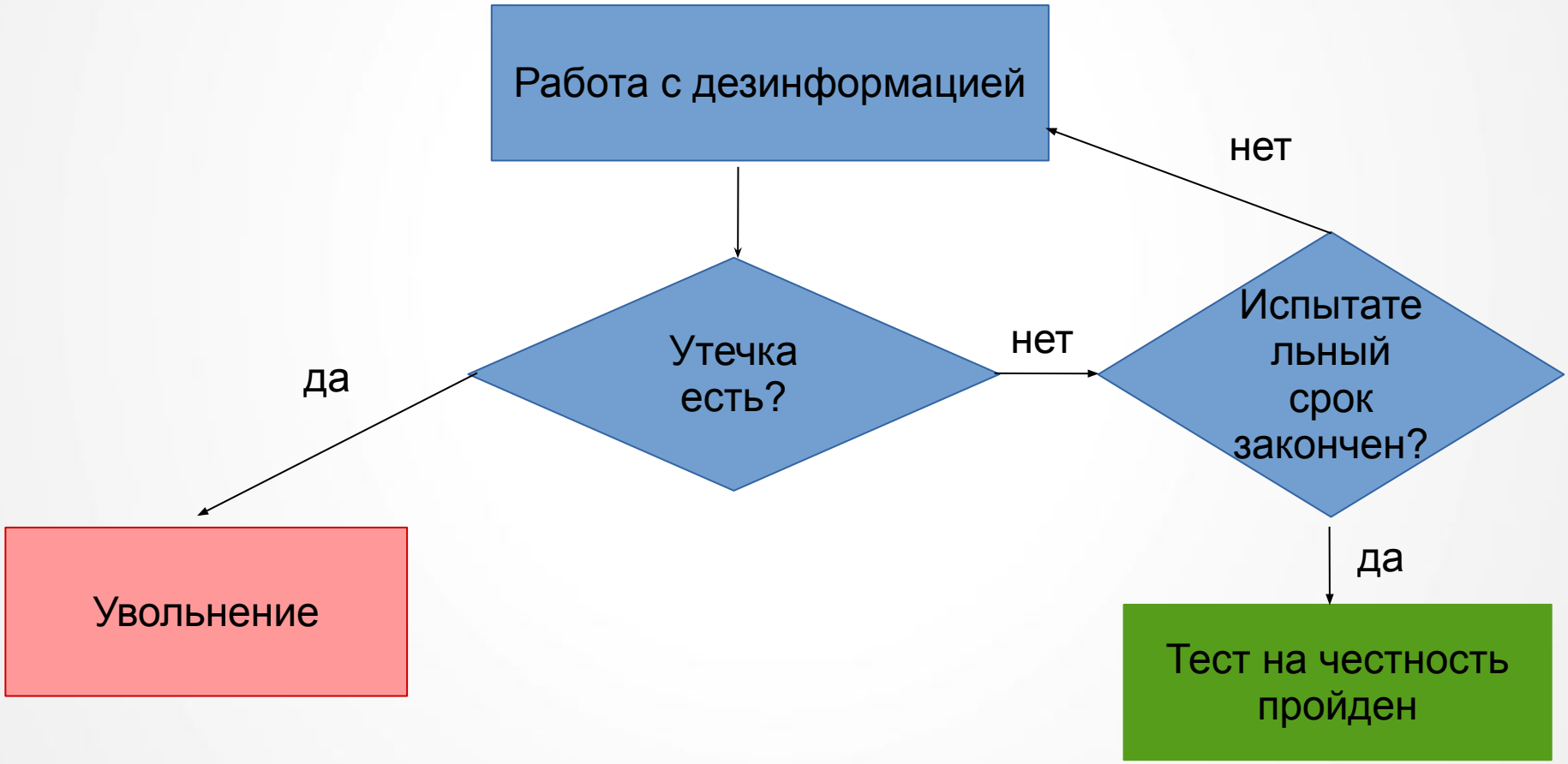
  Использование психолога для оценки личностных качеств.

Замечание: интервьюеру следует избегать длительной вступительной речи об организации или о самой работе, поскольку это может вызвать льстивые или определенным образом ориентированные ответы.

Преимущественные качества кандидатов

Качество	Значимость
Негативное отношение к алкоголю	Высокая
Низкая общительность и/или социофобия	Низкая
Негативное отношение к курению	Высокая
Реальная оценка планов на будущее	Высокая

Алгоритм тестирования



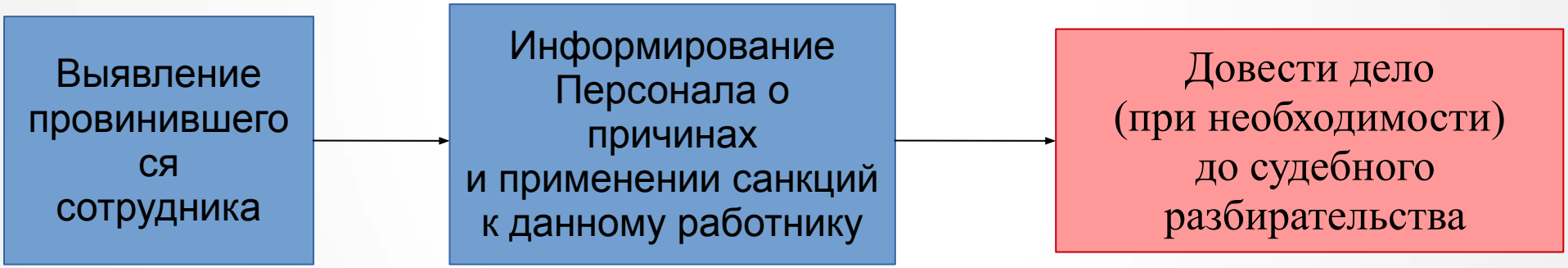
Мероприятия для сотрудников

Каждый сотрудник должен быть проинформирован, что его будут проверять на устойчивость к подкупу (необходимо прописать в договоре), а именно, периодически инсценировать попытку подкупа. Главное здесь - это добиться, чтобы потенциально уязвимый сотрудник считал настоящую попытку подкупа - проверкой, в случае провала которой его уволят за неудовлетворительный результат теста на лояльность.

Повышение лояльности работника

- Введение японской системы оплаты
- Поддержание благоприятной рабочей обстановки
- Введение системы преимуществ (оплата проезда, бесплатное питание в обеденный перерыв и т.п.)

Мероприятия повышения мер ответственности



Алгоритм рекомендаций по выявлению нарушителя

1 - изъять у сотрудника, предположительно открывшего канал утечки информации, все конфиденциальные сведения

2 - сменить направление деятельности подозреваемого сотрудника, не сообщая в причинах подозрения в утечке информации

3 - дезинформировать сотрудника в ходе его новой деятельности

4 - отследить возможный выход дезинформации из организации

5 - дополнительно: до окончания хода проверки, не доверять сотруднику конфиденциальных сведений

Увольнение сотрудника

По собственному желанию	Администрацией
• Не допускать нарушений корпоративной этики в отношении увольняющегося работника; • Не препятствовать уходу; • Не задерживать выплату; • Поднять моральную сторону вопроса.	• Вывести конфиденциальную информацию из использования; • «Сдвинуть» фокус внимания; • Поддержание лояльности; • Беседа со службой безопасности.

Предотвращение дальнейших увольнений

- Практика «обратной связи» в которой увольняющегося сотрудника просят написать отзыв об организации.
- Применение полученной информации.

Выводы

- выявлены причины известных уязвимостей человека, как носителя информации;
- разработаны и добавлены новые рекомендации приёма на работу;
- рекомендован новый порядок проведения испытательного срока;
- разработаны рекомендации в проведении контроля рабочего процесса сотрудников.
- Внедрение рекомендаций для тестового использования в ЗАО «Интегра-С»