



```
if (isset($_POST['login']) && isset($_POST['password'])) {  
    $db = mysql_connect('dbserver', 'user', 'password');  
    mysql_select_db($database);  
    $login = $_POST['login'];  
    $password = $_POST['password'];  
    $query = "SELECT login FROM users WHERE login='admin' and password='$password'";  
    $result = mysql_query($query);  
    if ($result) {  
        //proc...
```

```
public void doPost(HttpServletRequest request, HttpServletResponse response)  
    throws ServletException, IOException {  
        String query = "SELECT * FROM items";  
        List<Item> items = jdbcTemplate.query(query, new RowMapper<Item>() {  
            public Item mapRow(ResultSet rs, int rowNum) throws SQLException {  
                Item item = new Item(rs.getString("id"), rs.getString("name"), rs.getString("description"));  
                return item;  
            }  
        });  
        response.setContentType("application/json");  
        response.setCharacterEncoding("UTF-8");  
        PrintWriter out = response.getWriter();  
        out.println(items);  
    }  
}
```

БЕЗОПАСНОСТЬ В ЦИФРЕ

Хайретдинов Рустэм
Инфовотч

В цифре любая безопасность цифровая, но



- **За функционал** отвечает внутренний заказчик
- **За реализацию** функционала отвечают разработчики и внедренцы (свои или чужие)
- **За инфраструктуру** отвечает ИТ-департамент
- **За поддержку** клиентов - колл-центр
- **За безопасность** – служба информационной безопасности

Часто у них разные цели и критерии их достижения



Риски нарушения процессов

- Кибератаки
- Финансовое мошенничество
- Инсайд, торговля информацией
- Информационные атаки, fake news
- Воровство материальных активов
- Кражи секретов и интеллектуальной собственности
- Компьютерные сбои
- Ошибки в изменениях процессов
- Ошибки операторов и системных администраторов



Старый подход к безопасности не успевает

- Нет детального описания систем, не понятно, где сбой, а где плановое функционирование
- Много ложных срабатываний – велик риск остановить легальный процесс
- Уход в пассив - признание невозможности предотвращать угрозы и отражать атаки
- Рост расходов ресурсов на мониторинг
- «Кусочная» безопасность приводит только к увеличению расходов, эффективность которых нельзя посчитать



ТУПИК



Что изменяется в безопасности в «цифре»?

ОРГАНИЗАЦИОННО:

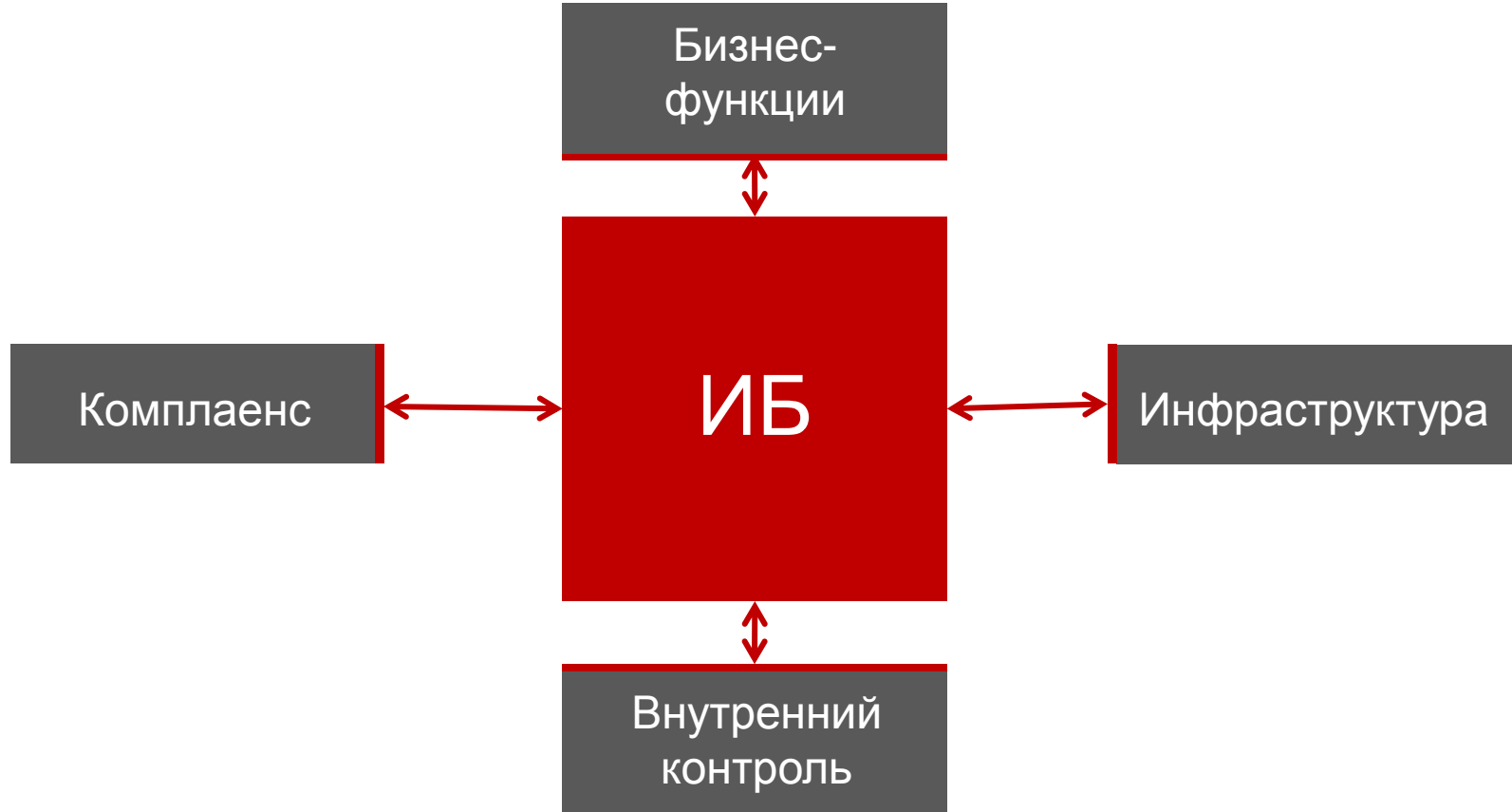
**ПОВЫШАЕТСЯ УРОВЕНЬ ОТВЕТСТВЕННОСТИ,
ОТВЕТСТВЕННОСТЬ КОНЦЕНТРИРУЕТСЯ В ОДНИХ РУКАХ**

ТЕХНИЧЕСКИ:

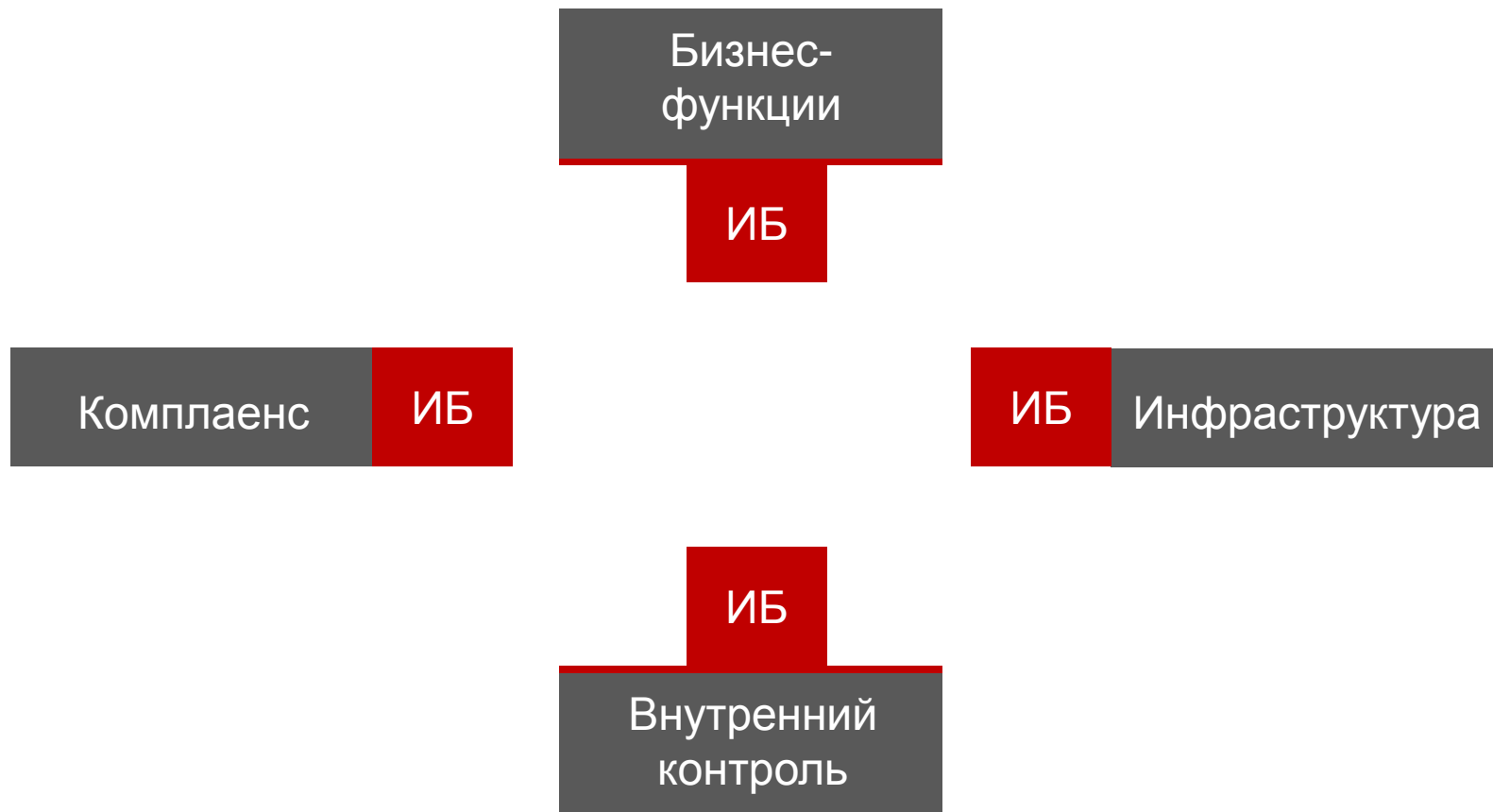
**Происходит переход от навесных
решений к встроенным,
интеграция в процессы с фокусом
на их устойчивость**

КОММУНИКАЦИОННО:

**Взаимодействие с бизнесом и
другими подразделениями**









```
public void doPost(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOException {  
    jdbcTemplate = new JdbcTemplate(dataSource);  
    String query = "SELECT * FROM items WHERE id=" + request.getParameter("id");  
    List rs = jdbcTemplate.query(query, new RowMapper() {  
        public Object mapRow(ResultSet rs, int rowNum) throws SQLException {  
            Item item = new Item();  
            item.setId(rs.getInt("id"));  
            item.setName(rs.getString("name"));  
            item.setDescription(rs.getString("description"));  
            return item;  
        }  
    });  
    response.setContentType("application/json");  
    response.setCharacterEncoding("UTF-8");  
    PrintWriter out = response.getWriter();  
    out.print(rsToJson(rs));  
    out.close();  
}
```

```
if (isset($_POST['login']) && isset($_POST['password'])) {  
    $db = mysql_connect('dbserver', 'user', 'password');  
    mysql_select_db($db);  
    $login = $_POST['login'];  
    $password = $_POST['password'];  
    $query = "SELECT login FROM users WHERE login='$login' and password='$password'";  
    $result = mysql_query($query);  
    if ($result) {  
        //process  
    }  
}
```

```
try {  
    List rs = jdbcTemplate.query("SELECT * FROM items WHERE id=" + request.getParameter("id"), new RowMapper() {  
        public Object mapRow(ResultSet rs, int rowNum) throws SQLException {  
            Item item = new Item();  
            item.setId(rs.getInt("id"));  
            item.setName(rs.getString("name"));  
            item.setDescription(rs.getString("description"));  
            return item;  
        }  
    });  
} catch (SQLException e) {  
    // обработка результатов  
}
```

```
try {  
    List rs = jdbcTemplate.query("SELECT * FROM items WHERE id=" + request.getParameter("id"), new RowMapper() {  
        public Object mapRow(ResultSet rs, int rowNum) throws SQLException {  
            Item item = new Item();  
            item.setId(rs.getInt("id"));  
            item.setName(rs.getString("name"));  
            item.setDescription(rs.getString("description"));  
            return item;  
        }  
    });  
} catch (SQLException e) {  
    // обработка результатов  
}
```

Спасибо за внимание!

Хайретдинов Рустэм
rustem@khairtdinov.com
+7 (903) 961-7312