OVODOV
CyberSecurity

Кибербезопасность с CEO

Тестирование на проникновение

Внешнее тестирование без доступа в инфраструктуру Заказчика.

Используемые модели тестирования:

- Черный ящик
- Серый ящик
- Белый ящик

Тестирование на проникновение

Уровень критичности	Уязвимость
Высокий	Выполнение произвольного кода на bitrixgram.test.ru
Высокий	Хранение привилегированных учетных данных на сетевом ресурсе
Высокий	Выполнение произвольного кода на bitrix24.test.ru
Высокий	Обнаружение конфигурационных файлов OpenVPN на скомпрометированном сервере bitrix24.test.ru
Высокий	Использование словарных паролей
Высокий	Компрометация контроллера домена test.ru
Высокий	Раскрытие конфиденциальной информации через веб-ресурс BitrixGram
Высокий	Открытая регистрация и публикация в базе знаний
Высокий	Хранимая XSS в редакторе статей базы знаний

Тестирование на проникновение

Уровень критичности	Уязвимость
Средний	Раскрытие информации о клиентах
Средний	Раскрытие персональных данных сотрудников
Средний	Получение состава команды по её идентификатору
Средний	Недостаточная проверка прав при приглашении участников
Средний	Массовая отправка одноразовых кодов через публичные API
Средний	Открытый просмотр содержимого каталогов
Средний	Возможность определения наличия пользователя в системе
Средний	Открытая документация API
Низкий	Публичный доступ к файлу логов
Низкий	Публичный доступ к Dockerfile
Низкий	Публичный доступ к внутренней документации
Низкий	Публичный доступ к конфигурации сервиса Vault
Низкий	Публичный доступ к файлу package.json

Тестирование на проникновение

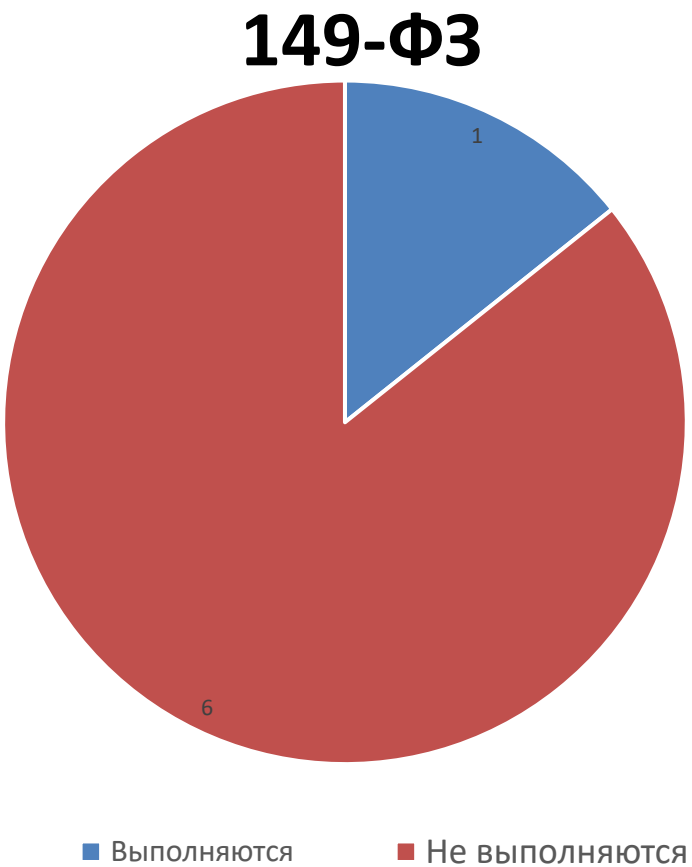
Результат

Возможность получения полного контроля над доменной инфраструктурой заказчика.

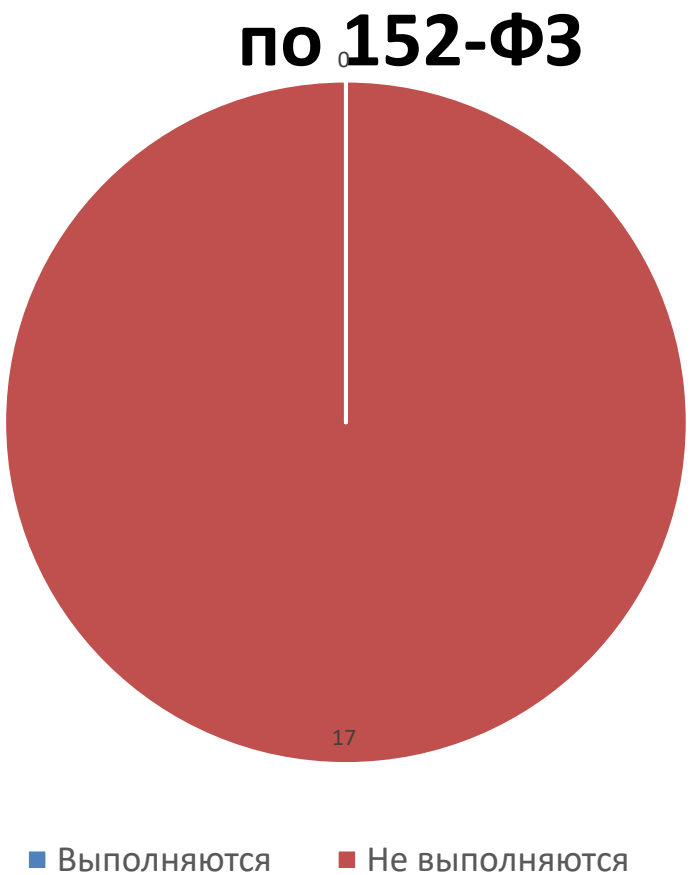
Аудит

- Изучение и анализ архитектуры локальной сети, настроек безопасности серверов и средств защиты информации
- Запрос и анализ локальных актов и документации регламентирующих процессы обеспечения ИБ
- Анализ численности подразделения ИБ к общему количеству сотрудников компании
- Проведение интервью с ИТ и ИБ специалистами
- Проведение интервью с ТОП и мидл менеджментом

Соответствие требованиям к защите информации по



Соответствие требования к защите персональных данных



Риски

№	Риск	Источник риска	Вероятность	Ущерб
1	Не уведомление Роскомнадзора о утечке персональных данных сотрудников (в случае ее выявления)	Взлом серверов баз данных, содержащих персональные данные и АРМ кадров и бухгалтера по заработной плате	Высокая	От 1 до 3 млн рублей
2	Полная потеря данных без возможности их восстановления	Взлом баз данных 1С и файлового сервера	Средняя	Порядка 30 млн рублей на восстановление данных
3	Потеря работоспособности ИТ инфраструктуры	Взлом средств управления ИТ инфраструктурой	Средняя	Порядка 3 млн рублей
4	Несвоевременное выполнение обязанностей по сдаче отчетности	Взлом серверов приложений 1С Бухгалтерия, 1С ЗУП; Отсутствие доступа к ЭДО	Средняя	От 500 рублей до 30% от размера налога или взноса подлежащих к уплате
5	Потеря потенциального дохода из-за неподачи заявки на участие в доходном тендере	Взлом АРМ с доступом к ЭТП; Отсутствие доступа в Интернет	Низкая	Зависит от суммы контракта – до 200 млн рублей прибыли
6	Несвоевременное выполнение обязанности по выплате заработной платы	Взлом серверов приложений 1С ЗУП	Низкая	Штраф до 50 000 рублей + Сумма Зарплаты*1/150* Ключевая ставка ЦБ
7	Задержка с подписанием договоров поставки материалов и оборудования	Отсутствие доступа к ЭДО	Низкая	Пени и штрафы по контактам с Клиентами за просрочку исполнения обязательства

Рекомендации по минимизации рисков информационной безопасности

OVODOV
CyberSecurity

Рекомендации по минимизации рисков.

Меры первого приоритета (реализация 1-3 месяца)

Сеть:

- Сегментация сети.
- Выполнение настроек безопасности сетевого оборудования.
- Обеспечение хранения резервных копий конфигураций сетевого оборудования.
- Обеспечение кластеризации сетевого оборудования (маршрутизатор и коммутатор ядра сети).

Инфраструктура:

- Организация доступа удаленных пользователей через терминальный сервер размещенный в DMZ.

Рекомендации по минимизации рисков.

Меры первого приоритета (реализация 1-3 месяца)

Сервера:

- Ограничение доступа к серверам на уровне операционной системы для пользователей.
- Использование отдельных учетных записей для доступа на АРМ и на сервера.
- Выполнить аудит структуры домена и выполнить его реорганизацию или осуществить переезд в новый домен.
- Настроить групповые политики домена.
- Выполнение настроек безопасности общесистемного ПО серверов.
- Использование 2хфакторной аутентификации для администрирования серверов, общесистемного ПО, и 1С.
- Реализация ежедневного резервного копирования с обеспечением наличие 4х резервных копий баз данных и ПО для восстановления серверной инфраструктуры:
  - ежедневная (хранение 14 последних дней);
  - ежемесячная;
  - ежеквартальная (по факту сдачи отчетности);

на 3х носителях

Бюджетная оценка. Первый этап

№	Наименование работ	Продукт	Бюджет, рублей
1	Приобретение ноутбука для резервного доступа к ЭТП и сдачи отчетности со средствами защиты информации	Ноутбук – 1 шт.	120000,00
2	Средство резервного копирования	Кибер Бэкап Платформа Виртуализации расширенная редакция – 1 шт.	300 000,00
		Съемный жесткий диск WD 4 ТБ – 5 шт.	80 000,00
3	Двухфакторная аутентификация администраторов на АРМ	Secret Net Studio 8 + Rutoken – 2 шт.	30 000,00
4	Проведение настроек безопасности на сетевом оборудовании, серверах и АРМ		
5	Кластеризация сетевого оборудования	Маршрутизатор – 1 шт.	65 000,00
		Коммутатор – 1 шт.	320 000,00
	ИТОГО		**915 000,00**

Рекомендации по минимизации рисков.

Меры второго приоритета (4-6 месяцев)

- Разработка Стандарта обеспечения информационной безопасности для Группы компаний
- Разработка документации по обеспечению защиты персональных данных (модель угроз безопасности, организационно-распорядительные документы, схема структурная системы защиты информации)
- Разработка документации по обеспечению информационной безопасности (политики, положения, планы мероприятий, инструкции, отчетные формы)

Бюджетная оценка. Второй этап

№	Наименование работ	Бюджет, рублей
1	Разработка документации по обеспечению защиты персональных данных (модель угроз безопасности, организационно-распорядительные документы, схема структурная системы защиты информации)	900 000,00
2	Разработка документации по обеспечению информационной безопасности (политики, планы мероприятий, инструкции, отчетные формы)	700 000,00
	ИТОГО УК	**1 600 000,00**

Рекомендации по минимизации рисков.

Меры третьего приоритета (7-12 месяцев)

- Реализация системы защиты персональных данных и проведение оценки соответствия
- Организация архитектурного комитета с включением в него специалиста по информационной безопасности и внешнего эксперта (заместителя директора по ИБ Управляющей компании (возможно на аутсорсинге)) с проведением обязательного согласования внедрения любых ИТ и ИБ продуктов в деятельность компании
- Организация проведения регулярного обучения сотрудников компании правилам и лучшим практикам обеспечения информационной безопасности (security awareness)

Бюджетная оценка. Третий этап

№	Наименование работ	Продукт	Бюджет, рублей
1	Реализация системы защиты персональных данных и проведение оценки соответствия	Точно будет определено по результатам проектирования системы защиты	До 1 000 000,00
	ИТОГО		**До 1 000 000,00**

Рекомендации по построению и обеспечению информационной безопасности в Группе Компаний

OVODOV
CyberSecurity

Состав рекомендаций

- 5 принципов обеспечения информационной безопасности
- Управление системами обеспечения информационной безопасности (СОИБ) дочерних обществ
- Порядок построения СОИБ
- Организационная структура подразделений информационной безопасности

Принципы обеспечения информационной безопасности

1. Стоимость СОИБ включая затраты на персонал не должна превышать стоимости защищаемой информации/ущерба от простоя в работе информационных систем.
2. При построении СОИБ фокус должен быть в первую очередь на защите данных, уничтожение которых может повлечь существенный ущерб для организаций группы и защите программного обеспечения и программно-аппаратных комплексов, нарушение работы которых повлечет за собой значительный ущерб.
3. Выполнение мер ИБ в первую очередь должно реализовывать за счет использования встроенных механизмов защиты программного и программно-аппаратного комплексов доступных для администрирования ИТ подразделению или возможных для передачи аутсорсинговой организации.
4. Принцип Парето - в первую очередь должны реализовываться меры защиты, которые при минимальных вложения дают максимальный эффект минимизации рисков ущерба.
5. Подчинение подразделений информационной безопасности дочерних обществ директору по безопасности или первому руководителю (ИБ не должно подчиняться ИТ)

Подход к управлению СОИБ

1. Найм или привлечение на аутсорсинге в УК заместителя директора по информационной безопасности отвечающего за эффективность обеспечения информационной безопасности в УК и дочерних обществах и соблюдение принципов
2. Создание единого стандарта обеспечения информационной безопасности для дочерних обществ, закрепляющего принципы, подходы, порядок построения и эксплуатации и управления СОИБ
3. Создание архитектурных комитетов по ИТ и ИБ в дочерних обществах группы с включением в нее заместителя директора по информационной безопасности УК
4. Соблюдение нижеуказанного порядка построения и эксплуатации систем обеспечения информационной безопасности

Порядок построения СОИБ в дочерних обществах Группы

1. Проведение первичного аудита
2. Формирование архитектуры СОИБ на основании оценки стоимости потери или утечки защищаемой информации, стоимости ущерба от недоступности ИТ систем, необходимости выполнения требований законодательства в области информационной безопасности
3. Разработка СОИБ с параллельной реализации первоочередных мер защиты
4. Реализация мер защиты необходимых для снижения ущерба до допустимого в случае инцидента и обеспечивающего приемлемое время восстановления работоспособности
5. Обеспечение эксплуатации ИТ и АСУ в соответствие с разработанной СОИБ

Организационная структура подразделений обеспечения информационной безопасности

1. Подразделения информационной безопасности подчиняются заместителю руководителя организации по безопасности или генеральному директору.
2. Подразделение информационной безопасности не входит в состав ИТ и не подчиняется ИТ.
3. Штатная численность подразделений определяется методологией, применяемой BCG.
4. Курирует работу подразделения ИБ заместитель руководителя УК по информационной безопасности/аутсорсинговый CISO.
5. Обеспечение информационной безопасности осуществляется в компаниях Группы в соответствие со Стандартом обеспечения информационной безопасности.