RTM GROUP

Как белые хакеры помогают защититься от реальных угроз?

Эксперт

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Федор Музалевский

Директор технического департамента RTM Group

Экспертная работа с 2010 года

Педагогический стаж с 2012 года

Кандидат физико-математических наук. Доцент кафедры ВМ и ИТ ФГБОУ ВО "ВГУИТ"

Артем Бруданин

Руководитель направления кибербезопасности

40 реализованных проектов по проектированию систем защиты и анализу защищенности

Автор патентов в сфере кибербезопасности и методик тестирования на проникновение

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Работаем на всей территории России, Беларуси и Казахстана, и не ограничиваемся на этом. Головной офис компании находится в Москве, производственное подразделение базируется в Воронеже.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

Информационная безопасность

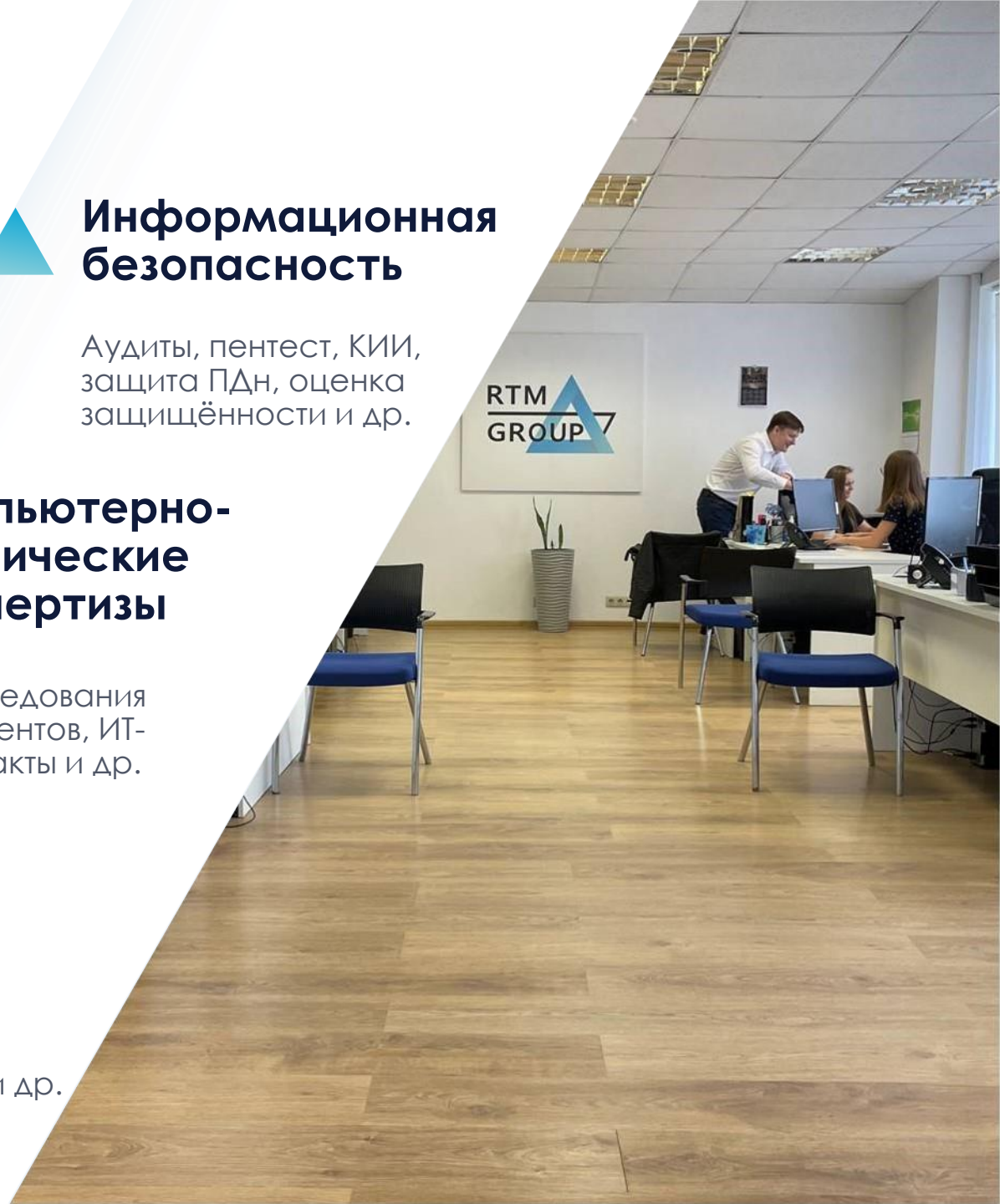
Аудиты, пентест, КИИ, защита ПДн, оценка защищённости и др.

Компьютерно-технические экспертизы

44-ФЗ, расследования инцидентов, ИТ-контракты и др.

ИТ-право

Судебное и досудебное урегулирование, сопровождение и др.



RTM GROUP

О чем пойдет речь

01 Безопасность технологических решений

02 Человек — самое слабое звено

03 (Не)безопасная разработка

04 Поставщики ИТ-услуг

05 Выявление недостатков мер защиты

06 Контроль Исполнителя

01. Безопасность технологических решений

1. Популярные технологии

Риски использования

Внедрение новых технологий повышает не только эффективность деятельности самой организации, но и эффективность, направленных против нее, компьютерных атак.

RTM GROUP

1.1 Популярные технологии

Как сделать современный технологический процесс более безопасным:

- Соблюдение методологий и принципов безопасного дизайна при использовании решений
- Объективный подход к политикам безопасности, не основанный на доверии к человеческому фактору
- Принцип минимально необходимых привилегий
- Внедрение технических и организационных мер защиты информации
- Внешний аудит ≠ внутренний анализ
- Периодическое повышение осведомленности сотрудников в области обеспечения ИБ
- Непрерывный контроль эффективности
- Не надеяться на «авось»

RTM GROUP

02. Человек — самое слабое звено

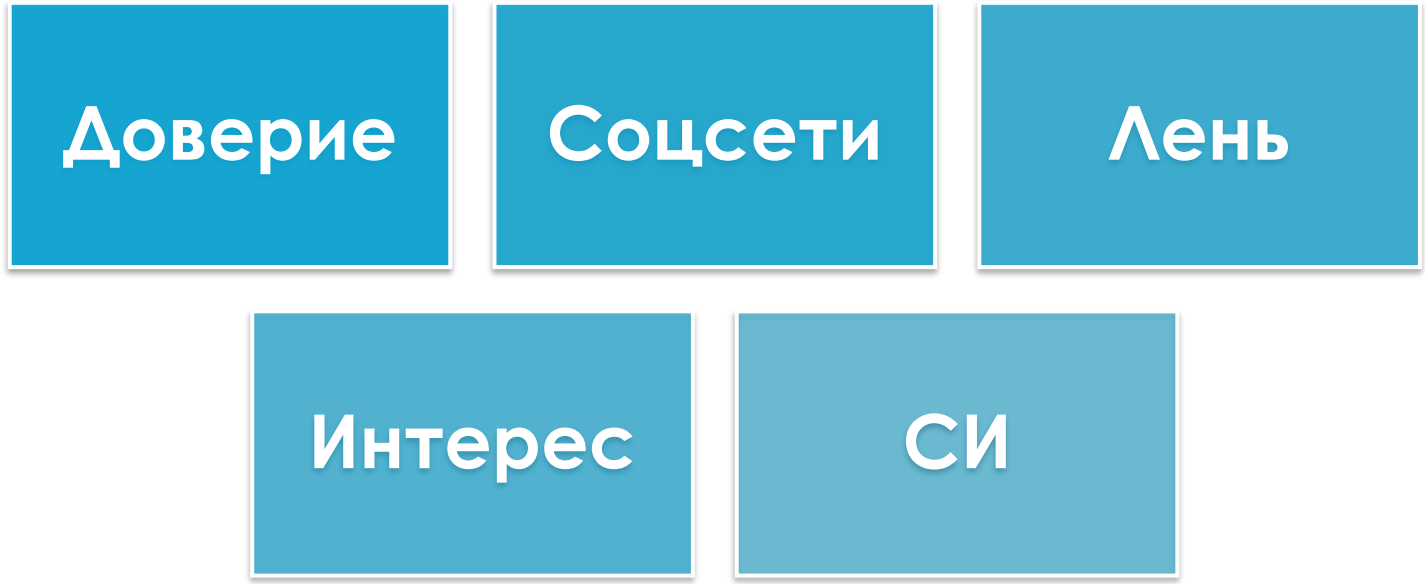
RTM GROUP

«Сегодня нет технологий, которые нельзя было бы победить с помощью социальной инженерии»

Фрэнк Абигнейл

2. Человеческий фактор

Ошибки людей в ИБ



2.1 Человеческий фактор

Как снизить влияние сотрудника на безопасность:

- Снова — принцип минимально необходимых привилегий
- Снова — объективный подход к политикам безопасности, не основанный на доверии к человеческому фактору
- Снова — внедрение технических и организационных мер защиты информации
- Снова — периодическое повышение осведомленности сотрудников в области обеспечения ИБ
- Снова — непрерывный контроль (в том числе и внешний)
- Придерживаться модели безопасности «нулевого доверия»
- Обучение технологиям, угрозам, тактикам и техникам злоумышленников
- Мотивация / отношения / убеждения / культура

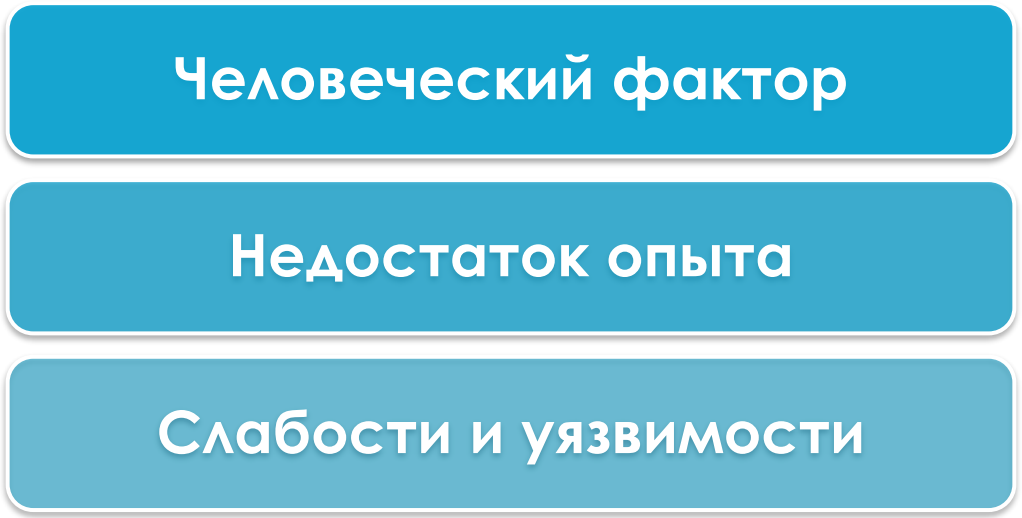
RTM GROUP

03. (Не)безопасная разработка

3. Разработка программного обеспечения

Связанные риски:

- Лень, некомпетентность, халтура, саботаж, месть и т.п.
- Недостаточные профессиональные навыки в области разработки безопасного ПО, несоблюдение стандартов DevSecOps
- CVE, CWE, CAPEC



3.1 Разработка программного обеспечения

Как снизить вероятность ошибок разработчика:

- Соблюдение «лучших практик» в области безопасной разработки и дизайна программного обеспечения
- Периодическое обучение и повышение квалификации команды разработки
- Непрерывный контроль качества исходного кода
- Внедрение автоматизированных средств аудита безопасности исходного кода
- Формирование команды тестирования продукта, использование юнит-тестирования
- Снова — работа с каждым разработчиком как с источником угроз человеческого фактора
- Привлечение внешних экспертов для объективной оценки
- Не экономить на хранилищах, серверах, инструментах и иных средствах обеспечения разработки

04. Поставщики ИТ-услуг

RTM GROUP

4. Чрезмерное доверие к поставщику ИТ-услуг

Нюансы и проблемы — что делать и куда смотреть

- Ответственность за обеспечение информационной безопасности
- Наличие средств защиты и их корректная конфигурация
- Разграничение прав доступа между «соседями»
- SLA («соглашение об уровне сервиса»)
- Резервное копирование
- Техническая поддержка
- Наличие слабостей или уязвимостей
- Возможность проведения анализа защищенности или тестирования среды функционирования

05. Выявление недостатков мер защиты

RTM GROUP

5. Анализ защищенности (поиск уязвимостей)

Процесс выявления всех известных уязвимостей в системном или прикладном программном обеспечении, используя автоматизированные или ручные сигнатурные и эвристические проверки.

+ Безопасно для данных и инфраструктуры
+ Относительно быстро и дешево
+ Можно выполнять часто, отслеживая изменения

– Не показывает реальную защищенность от целенаправленных атак
– Не выявляет недостатки бизнес-логики или конфигураций
– Зависит от используемой базы данных уязвимостей
– Зачастую потребуется отключение функционирующих средств защиты информации

RTM GROUP

5.1 Тестирование на проникновение

Процесс выявления слабостей и уязвимостей информационной системы путём моделирования и имитации действий потенциального злоумышленника — хакера.

+ Частично позволяет оценить защищенность инфраструктуры от целенаправленных атак
+ Позволяет выявить недостатки как бизнес-логики, так и конфигураций
+ Позволяет оценить не только техническую, но и социальную составляющую информационных систем
+ Сценарии тестирования разрабатываются под конкретную организацию

– Относительно долго и дорого
– Зависит от квалификации и опыта команды Исполнителя
– Потенциально небезопасно для данных и инфраструктуры
– Не получится делать часто

06. Контроль Исполнителя

6. Недобросовестный Исполнитель

Индикаторы

На что нужно обратить внимание при заказе услуг по анализу защищенности или тестированию на проникновение у внешнего Исполнителя, чтобы оценить эффективность и быть уверенным — ожидания соответствуют результату.

RTM GROUP

Мероприятия

@it_law_security

Вебинар: 757-П — новые требования для НФО от ЦБ

21 сентября в 12:00

Конференция: IT. Право. Безопасность. Online 2023

28 сентября в 10:00

регистрация

Спасибо за внимание!

Готовы ответить на Ваши вопросы


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


@RTM_Group


rtm.group


it_law_security