ACFE
Association of Certified Fraud Examiners
RUSSIA

2-я ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЗГЛЯД ИЗНУТРИ КОМПАНИИ»

7 февраля 2019г.

Учебный центр МБ Сбербанк,
г. Москва, 3й проезд Перова Поля, д.3а, аудитория 303, 3-й этаж.

09:00 - 09:30 **Регистрация**

09:30 - 09:40 **Открытие конференции**

09:40 - 10:10 Информационная безопасность как образ жизни.

Сергей Мартынов
Президент, российское отделение ACFE.

Для того, чтобы решить проблему информационной безопасности бизнеса, нужно радикально пересмотреть само понятие информации. Информация сегодня – это не последовательность битов или сигналов. Это нечто нематериальное, неосязаемое физически, находящееся неизвестно где, пронизывающее всё и всецело определяющее нашу жизнь.

Пространство в том месте, где вы сейчас сидите, пронизано парой десятков беспроводных сетей, которые постоянно передают о вас всё - о вашем каждом движении, вдохе и выдохе куда-то там. И если вы, не дай бог, чихнёте, вам тут же покажут рекламу лекарства от кашля. В лучшем случае. Информация циркулирует кругом, как воздух, которым мы дышим – в носимых фитнес-браслетиках, «умных» часах, смартфонах, всяких бытовых и не очень предметах интернета вещей. Поэтому традиционные методы и меры обеспечения ИБ работают всё хуже и хуже... Антивирус сейчас не более эффективен, как марлевая маска в чумном бараке.

Мы с вами обсудим новую парадигму информационного окружающего пространства и какое влияние она оказывает на задачу обеспечения информационной безопасности.

10:10 - 10:40 Практический опыт создания системы информационной безопасности в компании.

Антон Грунтов
Директор по безопасности, группа компаний Eqvanta.

В современной Компании все бизнес процессы завязаны на информационные технологии. При этом, традиционно, вопросам киберзащиты уделяется внимания, которого как правило, не достаточно. Вместе с тем, угрозы в киберсфере нарастают очень стремительно. Объектами устремления преступников становятся не только деньги, но и например, полная информация о функционировании бизнеса. Поэтому от грамотно выстроенной системы киберзащиты зависит успех всего предприятия.

На примере ГК Eqvanta мы рассмотрим опыт создания системы кибербезопасности. О проделанных в этом направлении шагах расскажет докладчик.

Ассоциация «Объединение сертифицированных специалистов по расследованию хищений»
www.acfe-rus.com ■ info@acfe-rus.org ■ +7 (495) 728-76-10

ACFE
Association of Certified Fraud Examiners
RUSSIA

2-я ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЗГЛЯД ИЗНУТРИ КОМПАНИИ»

7 февраля 2019г.

10:40 - 11:10 Построение систем информационной безопасности в современных условиях кибербезопасности.

Сергей Рысин
Эксперт по ИБ.

- Построение систем безопасности, целостность, доступность, конфиденциальность.
- Как понимается и как внедряется?
- Как выбирать продукты для решения задач?
- Почему архитектор ИБ и эксплуатант разные люди?

11:10 - 11:40 Круглый стол

11:40 - 12:10 Перерыв на чай/кофе

12:10 - 12:40 Возможно ли завершить внедрение DLP?

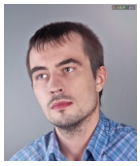
Дмитрий Шаронов
Ведущий специалист по ИБ, группа компаний Eqvanta.

3 года непрерывной настройки системы DLP. Красочные презентации вендоров и отрезвляющая реальность.

DLP системы уже далеко не самый свежий тренд, в связи с чем цены на них от года к году снижаются и все больше организаций начинает смотреть в их сторону как на возможность обеспечения зашиты от внутренних утечек информации при разумных вложениях. Но не многие до конца понимают, с какими трудностями и трудозатратами может быть сопряжено внедрение такого класса систем и только ли пользу они могут принести.

Из предлагаемого Вашему вниманию доклада Вы узнаете:
- На сколько нужно делить красочные обещания вендоров и интеграторов.
- Как оценить готовность Вашей инфраструктуры к внедрению DLP и понять, с какими проблемами Вы столкнетесь, если она не готова.
- Как юридически обосновать внедрение DLP и что делать, если пользователи ведут личную переписку с рабочих мест.
- Насколько важна формализация бизнес-процессов организации и какую она влияет на эффективность DLP.
- Что 95% ложных срабатываний – это не так уж и плохо и как не потонуть в ложных срабатываниях системы.
- Почему то, что мы хотим получить от системы и то, что она предоставляет – это разные вещи и как определиться с тем, что мы *действительно* хотим получить от системы.
- Что может пойти не так при плановом обновлении системы DLP и что Вам за это может сделать бизнес или как одна система может приостановить весь бизнес.
- Как понять, что Вы готовы перейти от мониторинга и реагирования к блокированию и разрешениям.
- О чем умалчивают вендоры и интеграторы или реальный опыт взаимодействия с технической поддержкой производителя системы.
- Как построить эффективную систему реагирования на инциденты.
- Как оценивать эффективность DLP в деньгах и доказать бизнесу, что вложения окупились.

12:40 - 13:10 Поиск «иголки» в «стогу сена». Анализ содержимого информационных потоков компании.



Андрей Сальников
Эксперт по ИБ

- Несмотря на впечатляющий объем потерь, связанных с хакерскими атаками, объем «потерь» (включая упущенную выгоду), связанных с деятельностью внутренних злоумышленников, во много раз больше.
- Единственный достоверный критерий поиска внутреннего злоумышленника – деятельность внутреннего злоумышленника, с которой связанны «потери» компании, является аномалией среди его повседневного поведения.

Ассоциация «Объединение сертифицированных специалистов по расследованию хищений»
www.acfe-rus.com ■ info@acfe-rus.org ■ +7 (495) 728-76-10

ACFE
Association of Certified Fraud Examiners
RUSSIA

2-я ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЗГЛЯД ИЗНУТРИ КОМПАНИИ»

7 февраля 2019г.

То есть большую часть времени работник все-таки посвящает исполнению должностных обязанностей и лишь иногда «пользуется служебным положением» в собственных интересах.
• Каким образом можно вычислить деятельность «внутреннего злоумышленника» на основе информации собираемой DLP, в случаях, когда данные действия не нарушают существующие регламенты компании?
• Можно ли находить признаки «злоупотребления служебным положением» на основе анализа информационных потоков?
• Как можно анализировать огромные объемы данных ограниченными ресурсами (в первую очередь: время и штат).

13:10 - 13:40 **Круглый стол**

13:40 - 14:25 **Обеденный перерыв (**не входит в стоимость участия.
На 2-м этаже здания находится кафе-столовая, где можно вкусно пообедать.)

14:25 - 14:55 **Интеграционные проекты: практические кейсы на основе собственного опыта.**

Елена Нагорная
Руководитель направления Департамента по защите активов и информации, Техснабэкспорт.

• С чего начинается любой интеграционный проект внедрения средств защиты информации;
• Какие основные этапы интеграционных проектов можно выделить и чему необходимо уделить особое внимание;
• Системная интеграция что это? И почему мы отдаем предпочтение такому виду внедрения систем/подсистем защиты информации;
• Как мы внедряли систему мониторинга событий ИБ (практический кейс, на что стоит обратить внимание при выборе SIEM систем).

14:55 - 15:25 **Интеллектуальные методы аудита кибербезопасности.**

Илья Трофимов
Исполнительный директор - начальник отдела аудита информационных технологий, Сбербанк

15:25 - 15:55 **Предпосылки, цели и задачи проведения Forensic-расследований. Инструменты проведения Forensic-расследований.**

Георгий Гусляев
Начальник управления защиты информационных ресурсов, ЧТПЗ.

• Сбор доказательств в электронном виде (выявление и восстановление информации).
• Обработка и анализ информации.
• Анализ информационных систем на наличие отклонений. Выводы.
• Какие должны быть результаты проведения расследований?

15:55 - 16:25 **Круглый стол**

16:25 - 16:45 **Перерыв на чай/кофе**

Ассоциация «Объединение сертифицированных специалистов по расследованию хищений»
www.acfe-rus.com ■ info@acfe-rus.org ■ +7 (495) 728-76-10

ACFE
Association of Certified Fraud Examiners
RUSSIA

2-я ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЗГЛЯД ИЗНУТРИ КОМПАНИИ»

7 февраля 2019г.

16:45 - 17:20 **Практика аудитов информационной безопасности.**

Максим Козлов
Начальник отдела ИТ аудитов, Блок внутреннего контроля и аудита, МТС.

- Стадии проекта по аудиту.
- Активности по проекту.
- Направления обследований (публичные сервисы, доступные из сети Интернет; сетевое оборудование; серверное оборудование; рабочие места сотрудников; мобильные устройства; операционные системы; базы данных; процесс управление доступом (на уровне приложений, БД, удаленный доступ, физический доступ к оборудованию, привилегированные пользователи, доступ внешних подрядчиков); используемое программное обеспечение; осведомленность в вопросах ИБ сотрудников; квалификация ИБ-персонала; используемые средства защиты информации (антивирусные системы, DLP-системы, криптографические средства, системы сетевой защиты (межсетевые экраны, IDS/IPS - системы, фильтрация трафика) и др.), наличие и актуализация нормативной документации).
- Наиболее распространенные файндинги.
- Практические кейсы.
  Инструментарий ИТ-аудита;
  Потенциальные сложности при проведении аудитов;
  Результаты и их использование.

17:20 - 17:55 **ИТ аудиторы как внутренние хакеры. Аудит безопасности АТМ (банкоматы).**

Владимир Лобас
Начальник Отдела аудита информационных систем аналитической поддержки, директор, Райффайзенбанк.

- В какой степени внутренние аудиторы могут выполнять роль внутренних хакеров.
- Актуальные риски в 2019 по исследованиям: PWC, Gartner, European institutes of internal auditors.
- Кейс №1. Поиск паролей в конфигурационных файлах.
- Кейс №2. Риски тестовых сред.
- Кейс №3. Базовые правила ИБ.
- Анализ аудитором сценариев риска. Путь от пароля до денежных потерь.
- Пути решения проблемы: единая система авторизации для приложений.
- Уязвимое место в банковской сети – банкоматы (АТМ).
- Банкомат как объект защиты от логических атак. Методы оценки защищённости.
- Презентация менеджменту организации итогов работы аудиторов.

17:55 - 18:00 **Закрытие конференции**

По не зависящим от Организатора причинам в программе могут быть незначительные изменения.
Организаторы приложат все усилия, чтобы этого не допустить.

Ассоциация «Объединение сертифицированных специалистов по расследованию хищений»
www.acfe-rus.com info@acfe-rus.org +7 (495) 728-76-10