Как организовать повышение осведомленности работников субъекта КИИ?

КОНСТАНТИН САМАТОВ

Члена Правления

Ассоциации руководителей служб информационной безопасности

Зачем нужны мероприятия по повышению осведомленности

Формальный аспект

ЗОКИИ

- Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (утв. приказом ФСТЭК России от 25 декабря 2017 г. № 239)
- Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСБ России от 19.06.2019 № 282)

ОКИИ

- Федеральный закона от 27.07.2006 № 152-ФЗ «О персональных данных»
- Требования по обеспечению защиты информации в автоматизированных системах управления технологическим процессом (утв. приказом ФСТЭК России от 14 марта 2014 г. № 31)
- Требования о защите информации в государственных информационных системах (утв. приказом ФСТЭК России от 11.02.2013 № 17)
- СТО БР ИББС-1.0-2014, ГОСТ Р 57580.1-2017 и иные нормативные акты по информационной безопасности в финансово-кредитной сфере

Прикладной аспект

- **По данным исследования Gartner, когда дело доходит до кибербезопасности, наиболее уязвимым местом организации являются её сотрудники, а не системы** (https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023)
- 85% утечек данных происходят из-за «человеческого фактора» (2021 Data Breach Investigations Report, Verizon). По данным ежегодного исследования «СёрчИнформ», в 2021 году 66% инцидентов в ИБ были неумышленными.
- 55% ИТ-руководителей ожидают, что сотрудники будут предупреждать их о киберинцидентах. При этом в 89% случаев вовлеченным в инциденты сотрудникам пришлось столкнуться с негативными последствиями этих инцидентов. Только у 54% работников обладают специальными профильными знаниями в области ИБ. (Egress Insider Data Breach Survey 2021)
- Ежедневно злоумышленники отправляют 3 млрд фишинговых писем (Email Fraud Landscape: Spring 2021, Valimail).
- Каждый четвертый сотрудник на работе открывал фишинговое письмо (Email Fraud Landscape: Spring 2021, Valimail).
- 63% руководителей высшего звена сообщили, что их сотрудники оставляли конфиденциальные документы в открытом доступе (Data Protection Report 2020, Shred-it).
- 57% сотрудников хранят пароли на стикерах на рабочем столе (Workplace Password Malpractice Report 2021, Keeper Security).
- Почти 24% людей использовали 1 в конце своего пароля (Unmasked: What 10 million passwords reveal about the people who choose them, WP Engine).
- 66% людей в основном или всегда используют один и тот же пароль (Psychology of Passwords, LogMeIn).
- 44% сотрудников повторно используют пароли в личных и рабочих учетных записях (Workplace Password Malpractice Report 2021, Keeper Security).
- 51% пользователей и 49% ИТ-специалистов иногда или часто делятся паролями с коллегами (The 2020 State of Password and Authentication Security Behaviors Report, Yubico).

Для каких групп работников проводить мероприятия по повышению осведомленности?

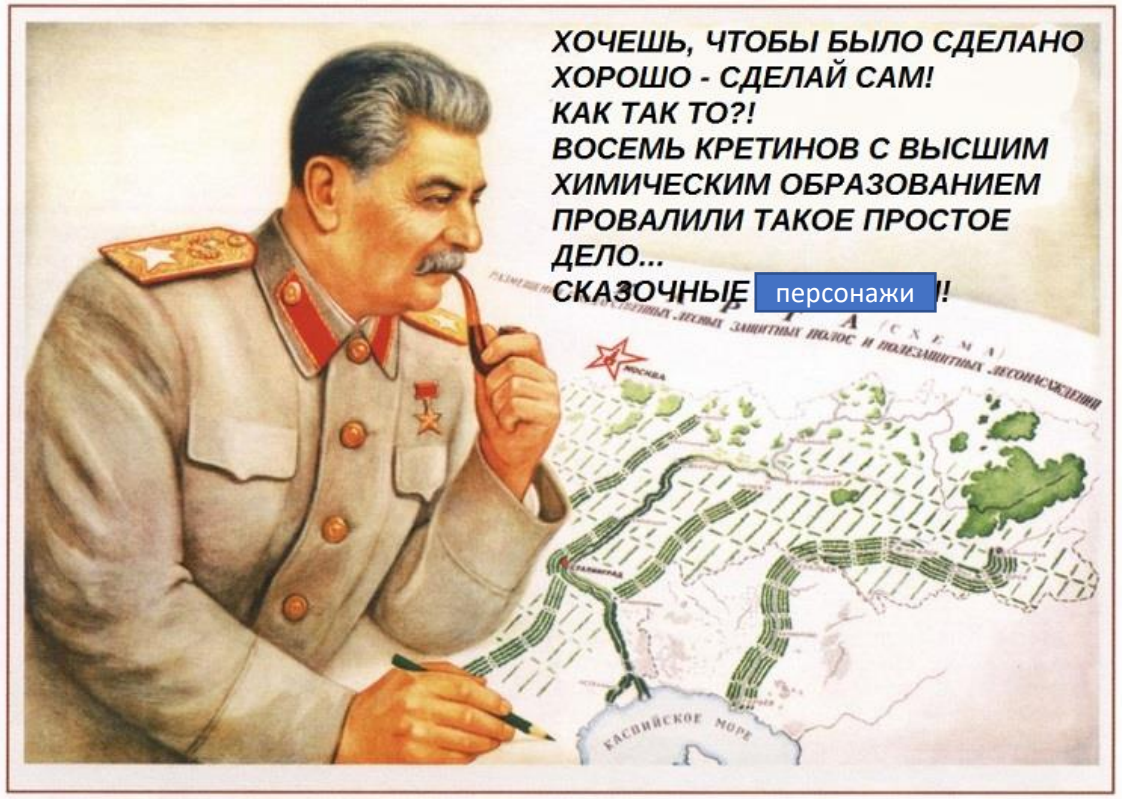
Категория	Мероприятия
Руководство (менеджмент)	Информирование о рисках и угрозах, их влиянии на бизнес Информационная рассылка Изменение законодательства по информационной безопасности
Работники эксплуатирующие информационные ресурсы (пользователи)	Информационная рассылка Обучающие курсы, тренинги Антифишинговые тренировки Киберучения (без отработки навыков на киберполигонах) Митапы (Meetup)
Работники, обеспечивающие функционирование информационных ресурсов	Информационная рассылка Обучающие курсы, тренинги Антифишинговые тренировки Киберучения (с отработкой навыков на киберполигонах)
Работники, обеспечивающие безопасность информационных ресурсов	Повышение квалификации Обучающие курсы, тренинги Изменение законодательства по информационной безопасности Киберучения (с отработкой навыков на киберполигонах), Red Teaming

Мероприятия по повышению осведомленности

- **Мероприятия**
  - Киберучения
    - Штабные
    - Командно-штабные
    - Антифишинговые тренировки
    - Red Teaming
    - Тренировка на киберполигоне
  - Митапы (Meetup)
  - Повышение квалификации
  - Обучающие курсы, тренинги
    - Внутренние
    - Внешние
  - Информирование о рисках и угрозах, их влиянии на бизнес
    - в виде коротких справок (формата one page only)
    - краткие презентации на совещаниях (формата pitch deck)
  - Информационная рассылка
    - Для ИБшников
    - Не для ИБшников
  - Изменение законодательства по информационной безопасности
    - Для руководства
    - Для всех работников

Как организовывать?

Самим



С привлечением специализированной компании

4	Криптография	- Основы криптографии - Ассиметричные, симметричные ключи. Хэши - Электронная подпись - Стеногрфия - Симметричные и ассиметричные криптосистемы

А

это темы обучения? даже если они опечатались и хотели написать "стеганография", то я всё равно не понимаю как это связано с криптографией))

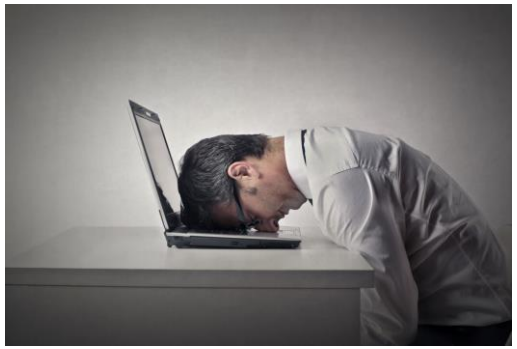
09:29

Содержание работ

КШТ проводится в соответствии с приведенным ниже основным сценарием (замыслом) тренировки. В одной из организаций ТЭК произошел инцидент информационной безопасности. Сотрудники служб информационной безопасности организации начинают расследование инцидента. На каждом этапе расследования обнаруживаются следы деятельности группировки злоумышленников, которые представляют собой определенные, но не всегда стандартные техники организации и проведения атаки. Участникам предстоит определить последовательный ход атаки, проанализировать, как и какими средствами можно предотвратить деятельность злоумышленников и как обезопасить себя в будущем от целевых атак кибергруппировок.

КШТ обеспечивает выполнение участниками следующих основных задач:

- ✓ определить тактики и техники, применяемые злоумышленниками;
- ✓ выявить слабые стороны киберзащиты и процессов обеспечения информационно безопасности в банке, приведшие к реализации инцидента злоумышленниками;
- ✓ оценить эффективность применяемых в настоящее время в банке средства и меры противодействия в приложении к представленному сценарию;
- ✓ оценить эффективность текущих процессов и мер противодействия в приложении к представленному сценарию;



Описание инфраструктуры

Предлагаемые объемы инфраструктуры вмещают в себя до 10 человек, что означает развертывание двух идентичных стандартных инфраструктур для проведения киберучений.

Спасибо за внимание!

КОНСТАНТИН САМАТОВ

Члена Правления

Ассоциации руководителей служб информационной безопасности