НТЦ ВУЛКАН

ПОДХОДЫ К ПОВЫШЕНИЮ ИБ-ОСВЕДОМЛЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ОБЪЕКТОВ КИИ

Владимир Алеев
заместитель директора по развитию

www.ntc-vulkan.ru

ПРЕДПОСЫЛКИ

Пользователь – один из самых уязвимых элементов современных ИС и АСУ, входящих в состав объектов КИИ

«ЧЕЛОВЕЧЕСКИЙ ФАКТОР»

По статистике более половины инцидентов ИБ происходят по вине пользователей, при этом более 80% этих инцидентов происходят из-за неумышленных действий

~ 30%

Повышать осведомленность пользователей объектов КИИ в области ИБ нужно для того, чтобы они:

- Понимали действующую политику ИБ
- Понимали роли и обязанности по обеспечению ИБ
- Знали и обладали навыками выполнения требований и процедур ИБ

«ЗНАТЬ, УМЕТЬ, ВЛАДЕТЬ»

НОРМАТИВНАЯ БАЗА

ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (п. 4 ст. 16)

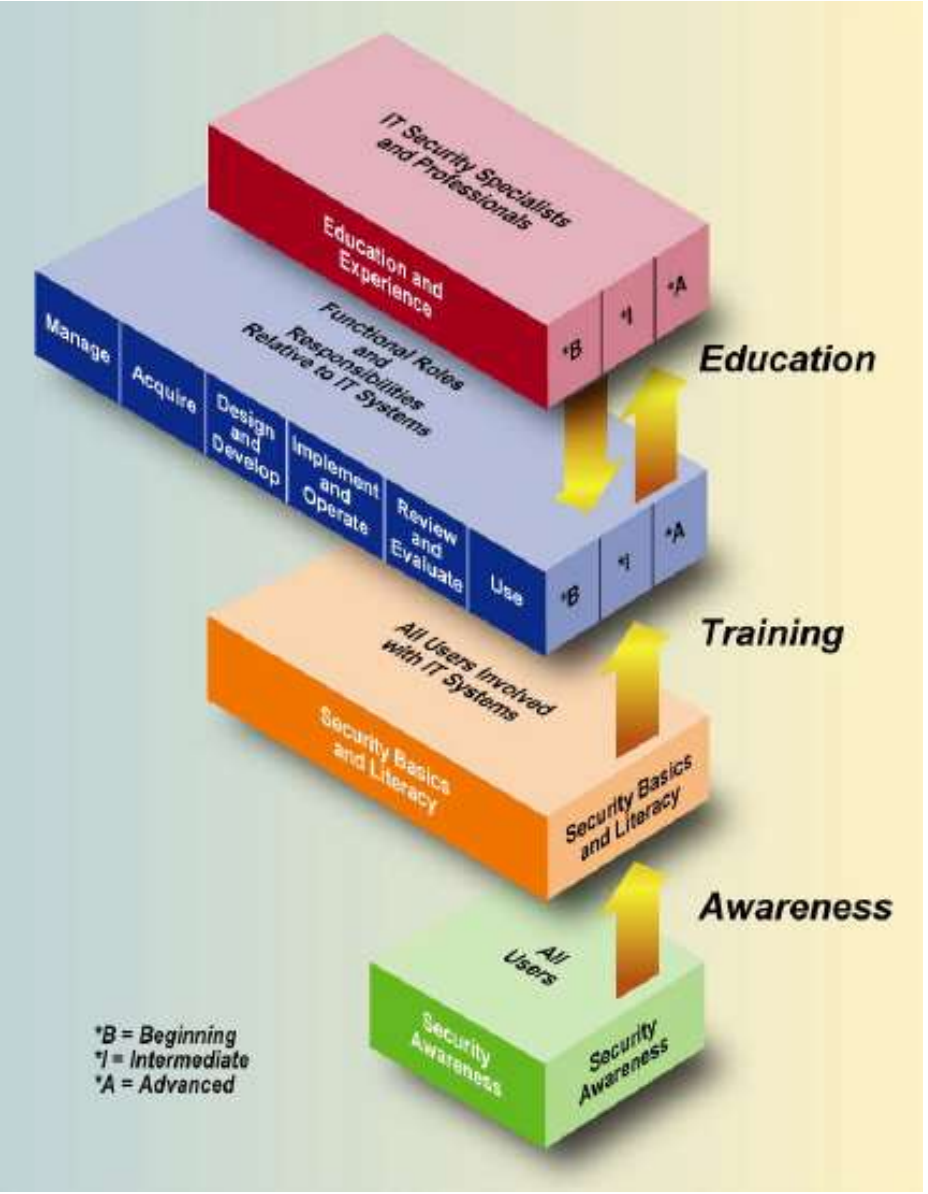
Решение аппарата Совета Безопасности Российской Федерации (март 2019 г.)

Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ» (ИПО.1 - ИПО.4)

Приказ ФСБ России от 06.05.2019 г. № 196 «Об утверждении Требований к средствам ГосСОПКА» (п. 13)

УРОВНИ ЗРЕЛОСТИ ПОДХОДА К ПОВЫШЕНИЮ ИБ-ОСВЕДОМЛЕННОСТИ

1. Система отсутствует
2. Комплаенс ориентированная система
3. Система, способствующая повышению осведомленности и изменениям поведения пользователей
4. Система долгосрочного характера, меняющая корпоративную культуру
5. Комплексная система с измеряемыми показателями



ЭТАПЫ СОЗДАНИЯ СИСТЕМЫ ПОВЫШЕНИЯ ИБ-ОСВЕДОМЛЕННОСТИ

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

ОБЩЕЕ ПОНИМАНИЕ

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

- Сколько пользователей целесообразно «натаскать» ?
- Каков их уровень сейчас ?
- На какие категории можно разбить персонал ?
- Какие инструменты информирования/обучения применить ?
- Кто будет отвечать за процесс ?
- etc.

НОРМАТИВНАЯ ОСНОВА

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

- Положение о повышении осведомленности…
- Программа повышения осведомленности…
- Внесение изменений в кадровые документы
- Приказы и распоряжения
- Изменение системы мотивации
- etc.

ОБУЧАЮЩИЕ И КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

– Запланировать и реализовать первичное массовое обучение и провести тестирование

– Запланировать и реализовать повторное тестирование (контрольные вопросы, проверка практических навыков с использованием техник социальной инженерии и киберучений)

– Регулярно информировать сотрудников по вопросам информационной безопасности

– Определить области ответственности, проработать порядок вовлечения руководителей подразделений в процедуры повышения и контроля уровня осведомленности

– На основании результатов первичной оценки осведомленности, результатов оценки осведомленности работников по итогам проведенного обучения определить цели и приоритеты таргетированного обучения

КРИТЕРИИ ЭФФЕКТИВНОСТИ

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

- Количество осознанных обращений пользователей по вопросам ИБ
- Доля пользователей, успешно прошедших «боевое» тестирование
- Временные затраты на достижение запланированного уровня
- etc.

РЕАЛИЗОВАТЬ ЗАПЛАНИРОВАННОЕ

- Сформировать общее понимание проблемы
- Разработать комплекс нормативных документов
- Спланировать обучающие и контрольные мероприятия
- Выработать критерии оценки эффективности
- Реализовать запланированное

Большинство обучающих мероприятий планируются и проводятся посредством автоматизированной системы, предназначенной для автоматизированного управления уровнем знаний сотрудников по вопросам информационной безопасности и выполняющей функции планирования, обучения и проверки знаний.

Это платформа для обучения с набором интерактивных курсов по тематикам ИБ. Используя коннекторы к различным информационным системам, решение выявляет пробелы в знаниях сотрудников и в автоматическом режиме направляет пользователя на соответствующий дистанционный курс с последующим тестом по изученному материалу.

РЕАЛИЗАЦИЯ АВТОМАТИЗИРОВАННОГО ПОДХОДА ПОЗВОЛИТ:

- Обеспечивать системное планирование и мониторинг эффективности мероприятий
- Осуществлять своевременное информирование, общее и тематическое обучение (для сформированных целевых групп персонала) в части корпоративных требований и процедур в области обеспечения информационной безопасности с использованием различных форматов обучающих мероприятий и форматов носителей информации
- Реализовывать контрольные процедуры по результатам обучения
- Поддерживать актуальность и развитие контента информирования и обучения
- Разрабатывать и внедрять меры стимулирования сотрудников к ответственности и лояльности при исполнении корпоративных требований в области информационной безопасности.

ПРЕИМУЩЕСТВА ПОДХОДА

- Стандартизация и унификация мероприятий в рамках процесса повышения осведомленности работников
- Расширение охвата работников информирующими, обучающими и контрольными мероприятиями
- Повышение контроля над уровнем осведомленности работников и оперативное выявление недостатков
- Оптимизация нагрузки на ответственные за повышение осведомленности подразделения и повышение эффективности мероприятий за счет автоматизации процессов.

СПАСИБО ЗА ВНИМАНИЕ!

НТЦ ВУЛКАН

www.ntc-vulkan.ru

marketing@ntc-vulkan.ru