IBS Platformix

ПОЧЕМУ ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЭТО ВАЖНО

Пушкина Светлана

Руководитель группы аудита и консалтинга
IBS Platformix

Содержание

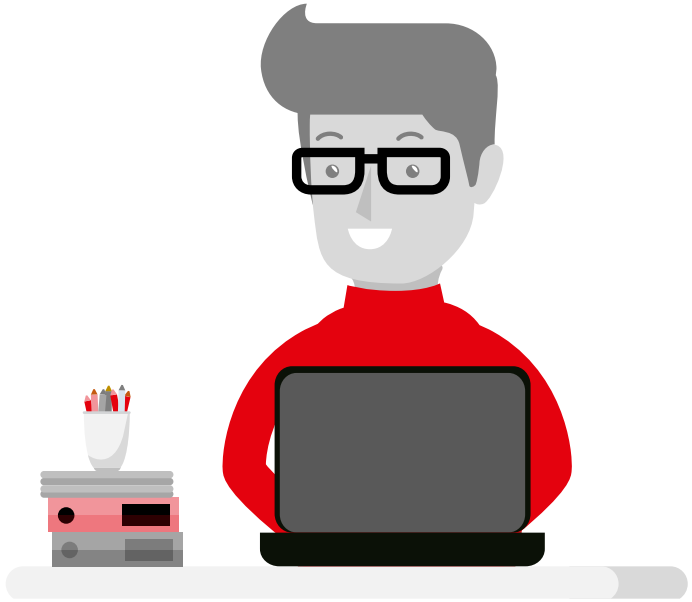
Светлана Пушкина
Руководитель группы аудита и консалтинга
IBS Platformix

IBS Platformix работает на российском ИТ-рынке с 1992 года и является дочерним предприятием компании IBS. Сегодня **IBS Platformix** – один из крупнейших системных интеграторов в России.

Специализация компании – тиражируемые решения для **корпоративной ИТ-инфраструктуры**.

С чем сталкиваются компании

БЕССИСТЕМНОСТЬ ПРОЦЕССА



Аудит по информационной безопасности в региональном офисе
Корректировка объема работ на инициирующей встрече

Запрос «проучить сотрудников»
Руководитель службы безопасности формулирует новую задачу

Рассылка фишинговых писем
«Все обязаны вакцинироваться в течение 5 рабочих дней или лишитесь годовой премии»

Во многих проектах есть блоки работ о повышении осведомленности, но это не системный процесс

Статистика атак

ПРОМЫШЛЕННОСТЬ

ТОП-3 отраслей по количеству атак

Основные методы атак

79% использование ВПО
51% социальная инженерия
45% хакинг

Статистика Positive Technologies в промышленном секторе в III квартале 2021 года

Объекты атак

Статистика Positive Technologies

Мировая практика

NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program

Отмечается, что учебный процесс является непрерывным. Он начинается с осведомленности, укрепляется на тренингах и формируется в рамках обучения

The new users guide: How to raise information security awareness

Распространяется на все сферы деятельности. На официальном сайте организации приведены видеоклипы, плакаты, иллюстрации и заставки на экран компьютера, способствующие повышению осведомленности по ИБ сотрудников организации

ISO/IEC 27001:2005

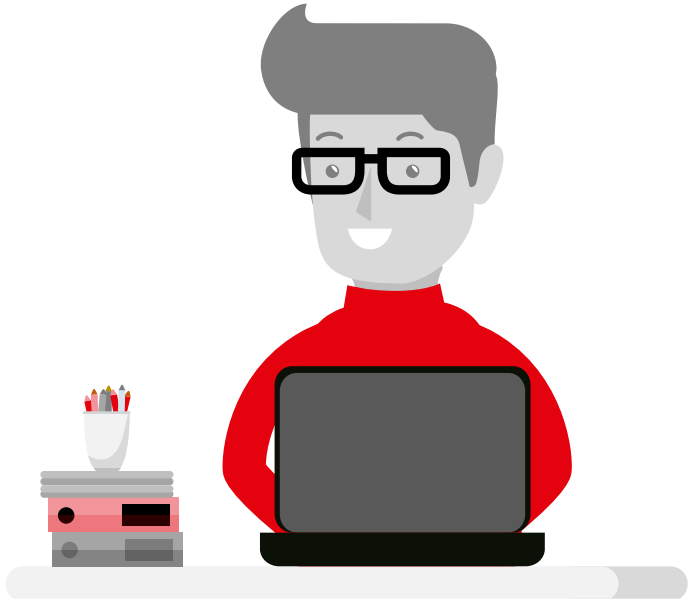
Подраздел 7.3. «Осведомленность» (Awareness), в котором приведены требования, что лица, осуществляющие работу под контролем организации, должны быть осведомлены о: политике информационной безопасности; своем вкладе в обеспечение эффективности системы менеджмента информационной безопасности, включая выгоды от улучшения функционирования информационной безопасности

Security Awareness Maturity Model

SANS Institute в 2011 году разработал «Модель зрелости осведомленности по вопросам безопасности» Модель зрелости Security Awareness определяет пять уровней зрелости процесса повышения осведомленности в сфере ИБ

С чем сталкиваются компании

ОТСУТСТВИЕ ЦЕНТРАЛИЗАЦИИ И МАСШТАБИРОВАНИЯ



Крупная компания с большой филиальной сетью
Компания придерживается мировой практики при построении СОИБ

Неравномерное распределение процесса
В главном офисе проводятся периодические обучения и даже киберучения, но региональные пользователи не осведомлены даже о том, что работают с конфиденциальной информацией

Отсутствие обучения порождает бреши в СОИБ
Региональные пользователи передают конфиденциальную информацию по открытым каналам связи

Столкновение лучших практик с российской территориальной действительностью

Российская практика

152-ФЗ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О персональных данных

В статье 18.1 пункт 1 подпункт 6: «Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами ...

98-ФЗ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О коммерческой тайне

1) Ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну
2) Ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности ...

№239

ПРИКАЗ ФСТЭК РОССИИ

Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Блок требований «XVII. Информирование и обучение персонала (ИПО)»

№31

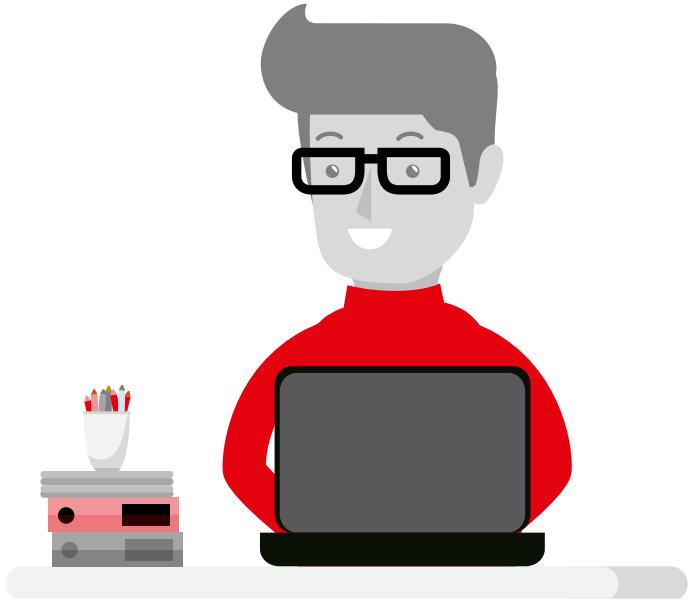
ПРИКАЗ ФСТЭК РОССИИ

Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах...

Блок требований «XVIII. Информирование и обучение персонала (ИПО)»

С чем сталкиваются компании

ОБУЧЕНИЕ РАДИ СООТВЕТСТВИЯ ЗАКОНОДАТЕЛЬСТВУ



Аттестация
Проект по переаттестации рабочих мест в государственном ведомстве

Соблюдение формальных требований
Все формальные требования соблюдены, в журналах стоят подписи

Отсутствие СЗИ на рабочих местах
«Не вижу у вас дополнительной системы аутентификации, как у вашей коллеги»

Требования регулятора против «русского авось»

Практика IBS Platformix

Модель зрелости Security Awareness определяет пять уровней зрелости процесса повышения осведомленности в сфере ИБ

Шаги для повышения уровня зрелости

КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ ПРОЦЕССА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ

Уровень зрелости	Наличие политик, регламентов	Периодичность обучения	Вовлеченность руководства	Автоматизация процесса	Визуализация и отчетность	Формат обучения	Восприятие службы ИБ	Корпоративная культура
1	—	—	—	—	—	—	Работники негативно относятся к службе ИБ	Работники никогда не обсуждают вопросы ИБ и не демонстрируют безопасное поведение
2	Политики разработаны, но не пересматриваются на регулярной основе	1раз в год	—	—	—	Регулярные рассылки подборок готовых материалов	Работники негативно относятся к службе ИБ	Работники считают, что ИБ - это формальность
3	Политики разработаны, но не пересматриваются на регулярной основе	1раз в квартал/полгода	Руководство понимает и признает необходимость управления человеческим фактором и обеспечивает поддержку	—	—	Фишинг	Работники уважительно относятся к службе ИБ	Работники сообщают об инцидентах ИБ или подозрениях на атаку
4	Политики пересматриваются и обновляются ежегодно	1раз в квартал+ Целевые группы	Руководство обеспечивает долгосрочную поддержку	Автоматизация отдельных операций в рамках процесса	Отдельная подсистема на основе специализированных решений	Киберучения, геймификация, Социотехническое тестирование на проникновение	Служба ИБ воспринимается как положительное явление	Работники запрашивают новости по безопасности/дайджесты и доп. информацию
5	Политики пересматриваются и обновляются ежегодно	1раз в квартал+ Целевые группы	Руководство обеспечивает долгосрочную поддержку	Автоматизация полного цикла процесса и интеграция с метриками инцидентов	Индивидуальные представления для разных типов пользователей	Проведение комплексных киберучений (Red/Blue Teaming)	Служба ИБ воспринимается как положительное явление	Руководство активно запрашивает и использует метрики осведомленности о безопасности для измерения их прогресса

ЖЕЛАЕМЫЙ УРОВНЕНЬ ЗРЕЛОСТИ МОЖЕТ БЫТЬ ОПРЕДЕЛЕН ИНДИВИДУАЛЬНО ДЛЯ КАЖДОЙ ХАРАКТЕРИСТИКИ

С чем сталкиваются компании

БЕССИСТЕМНОСТЬ ПРОЦЕССА

ОТСУТСТВИЕ ЦЕНТРАЛИЗАЦИИ И МАСШТАБИРОВАНИЯ

ОБУЧЕНИЕ РАДИ СООТВЕТСТВИЯ ЗАКОНОДАТЕЛЬСТВУ

ОГРАНИЧЕНИЕ БЮДЖЕТОВ И РЕСУРСОВ

НЕПОНИМАНИЕ ЦЕННОСТИ ИНФОРМАЦИИ

СЛОЖНЫЙ И НЕПОНЯТНЫЙ ПРОЦЕСС

ECSM slogan

IBS Platformix

Спасибо за внимание!

Thanks Merci Danke Mahalo ありがとう