

Вопросы информационной безопасности при цифровизации образовательного учреждения



Докладчик:
Юрий Горбунов,
Заместитель начальника управления
цифровой трансформации,
Пермский Политех



- один из ведущих многопрофильных инженерных вузов России
- один из лидеров рейтинга востребованности среди инженерных вузов (по данным МИА «Россия сегодня»)
- в числе ведущих научных и образовательных организаций РФ, имеющих право самостоятельного создания диссертационных советов и присуждения ученых степеней кандидатов и докторов наук
- обладатель гранта программы Приоритет 2030





- Увеличение количества атак с использованием шифровальщиков
- Цель большинства атак – нарушение основной деятельности, получение конфиденциальной информации
- У организаций крадут ПДн, основной канал – e-mail (фишинг, вредоносное ПО), компрометация оборудования
- У частных пользователей – учетные данные и ПДн, через сайты, соцсети, почту..
- Массовые утечки данных





- Подтверждение уничтожения персональных данных (акт и/или выгрузка журнала регистрации событий ИС)
- Уведомление о намерении осуществления трансграничной передачи ПДн
- Уведомление об изменении сведений об обработке персональных данных – до 15 числа следующего месяца
- Оценка вреда, который может быть причинен субъектам ПДн
- Уведомление об инциденте и результатах внутреннего расследования





- Инвентаризация данных и потоков
- Контроль ПДн, потоков и процессов обработки - от создания до уничтожения
- Реестр согласий, изменения согласий, отзывов, фактов передачи ПДн
- Уничтожение и обезличивание данных без упущенных возможностей
- Переход от формальных процессов к реальным действиям/изменениям





- Ограничения по использованию мессенджеров (ч.8 ст.10 N 149-ФЗ) – ПДн, платежи
- Ужесточение требования к владельцам хостинга - Госсопка, идентификация клиентов, взаимодействие с органами
- Введение машиночитаемых доверенностей
- Способы авторизации пользователей с 01.12.2023 – номер телефона, ЕСИА, ЕБС, иная система (владелец - гражданин РФ без иного гражданства или юр.лицо РФ)



- Потребность в IDM (Identity Management) системе - централизованное управление учетными записями и правами пользователей
- Проверка паролей на наличие в утекших базах
- Многофакторная аутентификация в сочетании с единой точкой входа (single sign-on), дифференцированная в зависимости от сервиса и уровня доступа к нему
- Контроль действий привилегированных учетных записей



Методические рекомендации по обеспечению информационной безопасности при создании и эксплуатации открытых репозиториях программного обеспечения

- Оператору рекомендуется реализовать:

11.4. сетевую защиту инфраструктуры открытого репозитория программного обеспечения (включая межсетевое экранирование, обнаружение и защиту от вторжений, защиту от атак типа «отказ в обслуживании»)

11.5. применение средств антивирусной защиты для проверки загруженных в открытый репозиторий программного обеспечения программных проектов;

11.7. периодический контроль уязвимостей информационной инфраструктуры открытого репозитория программного обеспечения;





IV. Меры по обеспечению информационной безопасности программного обеспечения, размещаемого в открытом репозитории программного обеспечения

Оператору рекомендуется реализовать, в т.ч. возможно на платной основе:

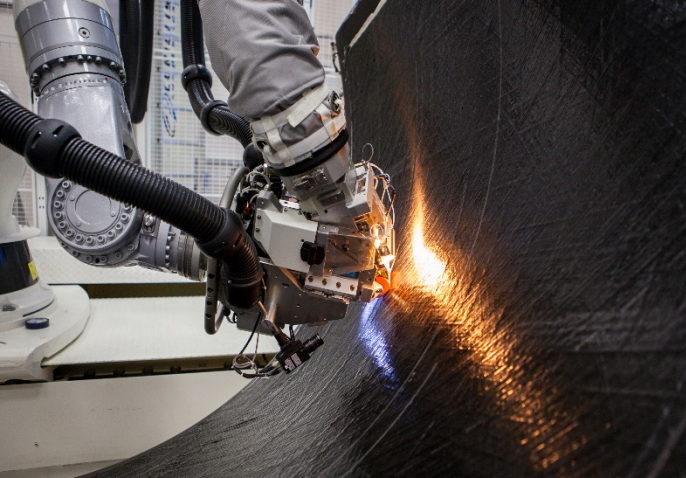
- 19.1. сервис тестирования программного обеспечения на уязвимости.
- 19.2. сервис по выявлению уязвимостей программных проектов
- 19.4. сервис публикации отчетов о безопасности программного обеспечения



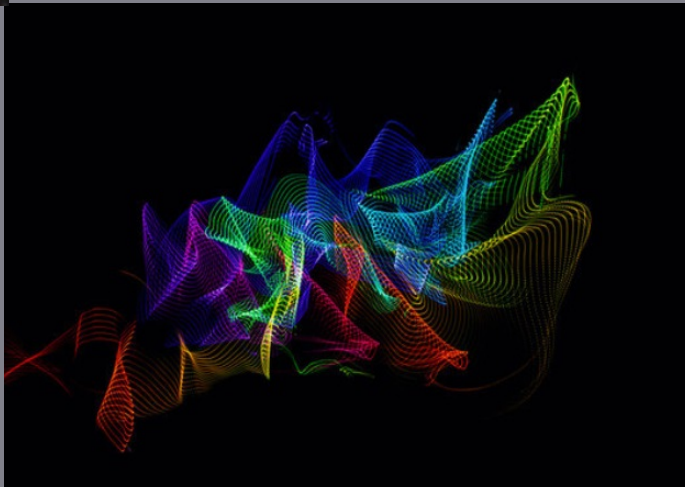


- Повод оценить и пересмотреть роль кибербезопасности во всех процессах
- Возможность предусмотреть, изменить, трансформировать
- Возможность получить необходимые ресурсы, будь то решение Security-by-Design или выстраивание системы кибербезопасности
- Возможность организовать обучение сотрудников





Спасибо
за внимание!



Юрий Горбунов,
Заместитель начальника управления
цифровой трансформации,
Пермский Политех
Контакты: +7 (342) 2-198-537,
yuri.gorbunov@pstu.ru