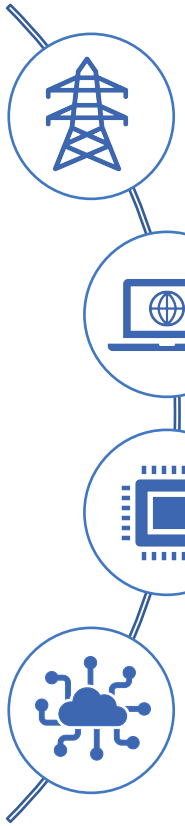
Элемент

Превентивная защита от кибератак в эпоху информационной войны

Александр Дворянский

Текущая ситуация в информационном поле. Всеобщая цифровизация



Телекоммуникационные сети - мобильный интернет, беспроводная связь, широкополосный доступ

Компьютерные технологии - компьютеры, ноутбуки, планшеты, смартфоны

Программная инженерия - операционные системы, программное обеспечение

Современные средства взаимодействия - электронная коммерция, медиаплатформы, социальные сети, мессенджеры

Сферы цифровизации

Политическая - безопасность, государственное управление, общественные организации, государственные службы, выборы, референдумы

Экономическая - компании, банки, деньги, сельское хозяйство, промышленность, торговля товарами и услугами

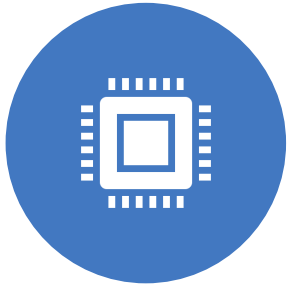
Социальная сфера - образование, здравоохранение, социальное обеспечение, социальные сети

Духовная - туризм, спорт, наука, медицина, развлечения, культура, искусство

Поле информационной войны

Инфраструктура систем жизнеобеспечения государства и Компаний - телекоммуникации, транспортные сети, электростанции, банковские системы.

Промышленный шпионаж - хищение патентованной информации, искажение или уничтожение особо важных данных, услуг; сбор информации разведывательного характера о конкурентах.



Цифровой след - взлом и использование личных паролей, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;

Электронные процессы компаний и различного рода сервисов – дезинформация и введение в заблуждение больших групп пользователей недостоверной информацией, зачастую политического характера.

Технические операции

Уничтожение, искажение или хищение информационных массивов данных;

Дезорганизация работы технических средств, телекоммуникационных сетей;

Остановка деятельности различного рода компаний.

Портрет злоумышленника

Основной мотив — деньги.

Широкий охват жертв и высокая вариативность преступных схем.

Готовые инструменты для преступлений, за счет чего большее вовлечение в преступный бизнес огромного количества людей, в т.ч. несовершеннолетних.

Миграция традиционных преступлений в Интернет.

Организатор преступной схемы редко сам занимается мошенничеством. Он создает условия, закупает инструменты и вербует исполнителей, которые будут работать на него, даже не зная его имени.

Реагирование на атаки

Способы и принципы определения ключевой информации в глобальном информационном пространстве

Проверьте несколько источников, оцените автора и комментарии к новости;

Сохраняйте критическое мышление и прислушивайтесь к собственным убеждениям;

Воспользуйтесь специализированными сайтами проверки фактов;

Получайте информацию только из проверенных источников;

Не пересылайте и не публикуйте информацию, в которой не уверены;

Злоумышленники используют громкие инфоповоды для своих корыстных целей;

Технические и организационные средства защиты

Организационные меры:

- Локально-нормативные акты.
- Корпоративное обучение.
- Имитация атак.
- Регулярное тестирование.
- Информирование о новых угрозах и методах их нейтрализации: рассылки, браузерные игры, геймификация.

Технические меры:

- Грамотно выстроенная инфраструктура Компании
- Внедренные и работающие процессы информационной безопасности
- Использование средств защиты информации на всех уровнях

Последствия информационной войны

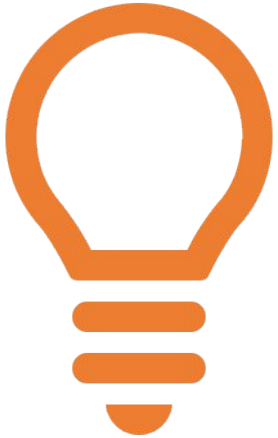
Финансовые потери

Репутационный ущерб

Штрафы за нарушение законодательства

Судебные иски от пострадавших клиентов

Выводы и рекомендации



- Повышать уровень компьютерной грамотности;
- Информировать о новых угрозах и методах защиты;
- Внедрять системы мониторинга на предмет цифровых рисков;
- Ужесточать наказание за киберпреступления и утечки информации.