Презентация на тему: «Мошенничество и киберпреступность».

Работу выполнили студенты группы
С8118-10.05.01-1СПЕЦ
Кваша А.С.
Бондарь А.Е.
Макаренко О.Р.

План

1) Таргетированные или целевые кибератаки.
2) Вирусы-шифровальщики.
3) Тенденции развития киберпреступности.
4) Вывод.

Тагретированные атаки – в тихом омуте черти водятся

КОМПЛЕКСНЫЕ

Злоумышленники используют сложные методологии для компрометации цели

ДОЛГОВРЕМЕННЫЕ

Злоумышленники работают медленно и скрытно, их основная цель - не быть обнаруженными как можно дольше

УГРОЗЫ

Злоумышленники целенаправленно выбрали Вашу организацию: они охотятся за критически важной для Вас информацией. Они хорошо подготовлены, организованы, мотивированы и не испытывают недостатка в средствах

ТАРГЕТИРОВАННАЯ АТАКА

КТО ЗЛОУМЫШЛЕННИК?

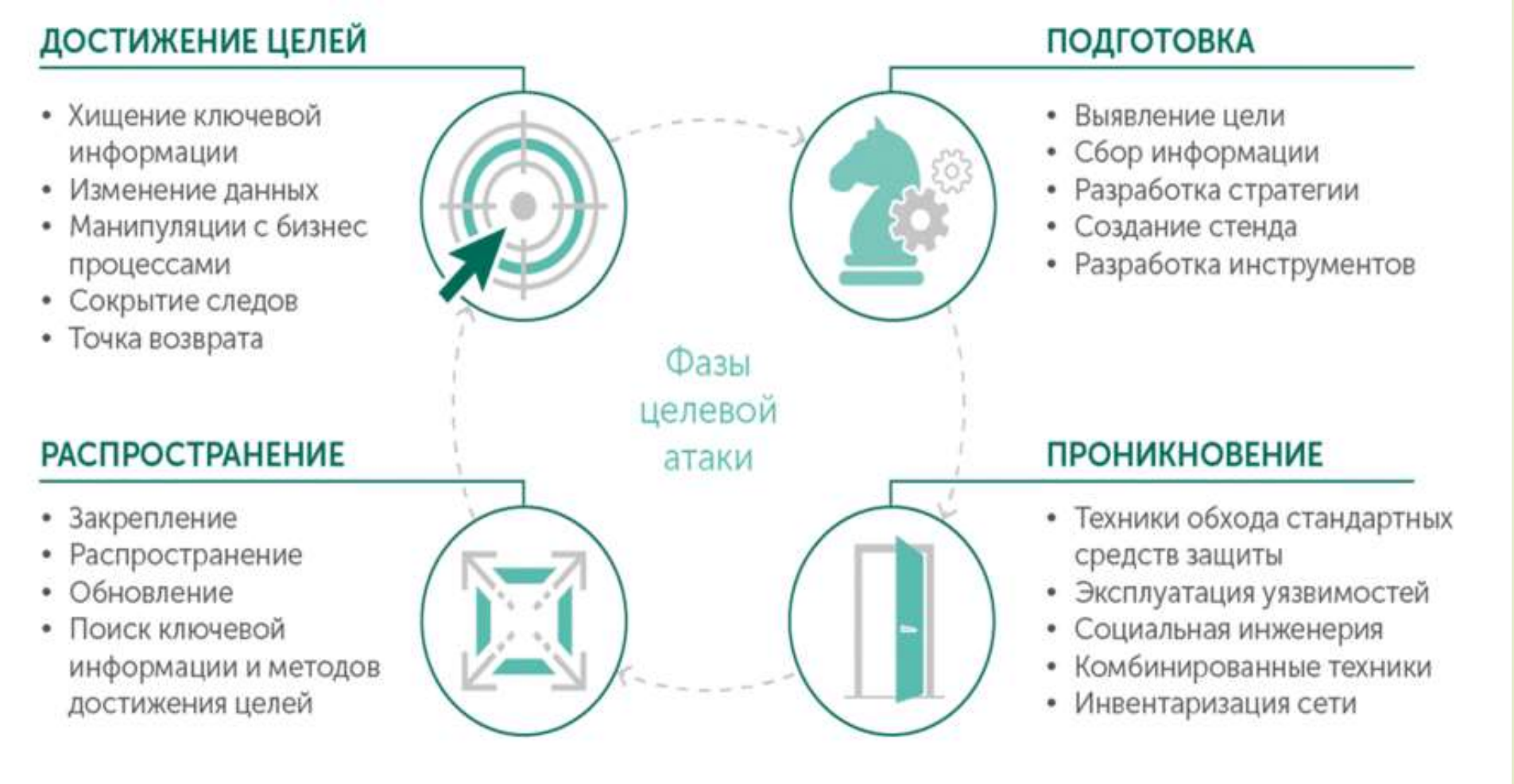
- Энтузиасты
- «Обиженные» сотрудники
- Организованные преступные группировки

НЕТАРГЕТИРОВАННАЯ АТАКА

КТО ЗЛОУМЫШЛЕННИК?

- Любители
- «Скрипт-школьники»

Атаке быть, вам не выиграть

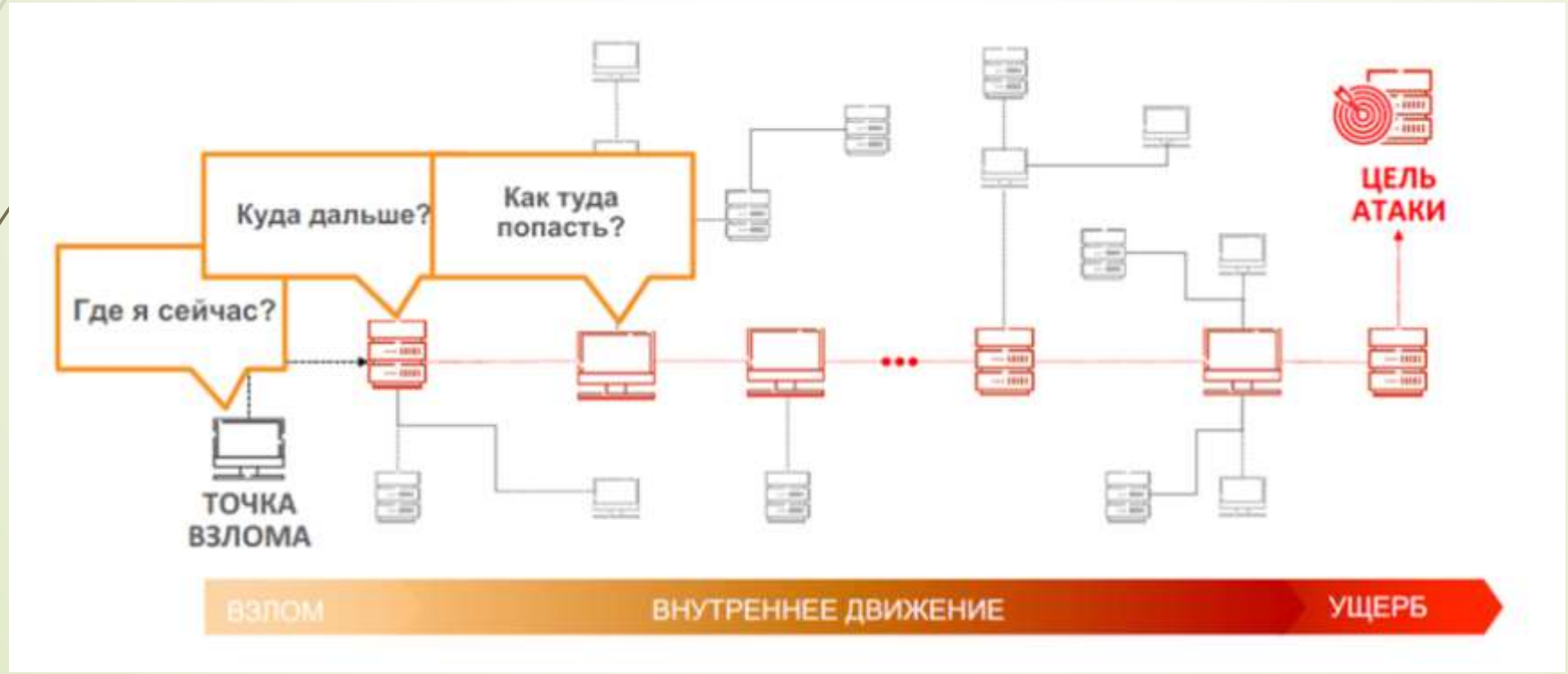


Deception-ловушки – главный инструмент борьбы

ПРИВЛЕКАТЕЛЬНАЯ ЛОВУШКА
ЦЕЛЬ: Отвлечение внимания злоумышленников

РЕАЛИСТИЧНЫЕ КОПИИ ИНТЕРЕСУЮЩИХ ЗЛОУМЫШЛЕННИКОВ ОБЪЕКТОВ
ЗАДАЧА: Направить злоумышленника по ложному следу

СИСТЕМА МОНИТОРИНГА
РЕЗУЛЬТАТ: Фиксация всех действий злоумышленника



Статистика или ее отсутствие

Киберпреступность

Киберпреступность - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж
- Атаки программ-вымогателей
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Вирусы-Шифровальщики

Программы-шифровальщики относятся к классу троянцев-вымогателей — это вредоносное ПО, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкупа).

40B$

оценивается мировой ущерб, ожидаемый в 2020 в связи с выплатой выкупов вымогателям и простоями [1]

x23

в 23 раза затраты, связанные с простоями, превышают среднюю сумму требуемого выкупа (по данным исследования [2])

141K$

Составлял средний ущерб из-за простоев в связи с атаками программ-вымогателей в 2019 г. (на 200% больше, чем в 2018 г.) [3]

62,4%

компаний подверглись атакам программ-вымогателей (по данным глобального опроса IT-директоров в 2019 г. [4])

22

новых семейства программ-вымогателей и 46 156 модификаций шифровальщиков было выявлено исследователями [6]

49%

атак вымогателей в I квартале 2020 г. проводились с использованием шифровальщиков [7]

Как защититься от шифровальщиков?

- Регулярно делать резервные копии данных, чтобы их можно было восстановить в случае инцидента.
- Использовать инструменты для автоматического обнаружения уязвимостей и установки исправлений.
- Своевременно обновлять приложения и операционные системы на всех устройствах.
- Не открывать подозрительные файлы или ссылки в электронных письмах.
- Установить на компьютер антивирус
- Скачивать программы только с сайта разработчика или с проверенных ресурсов.

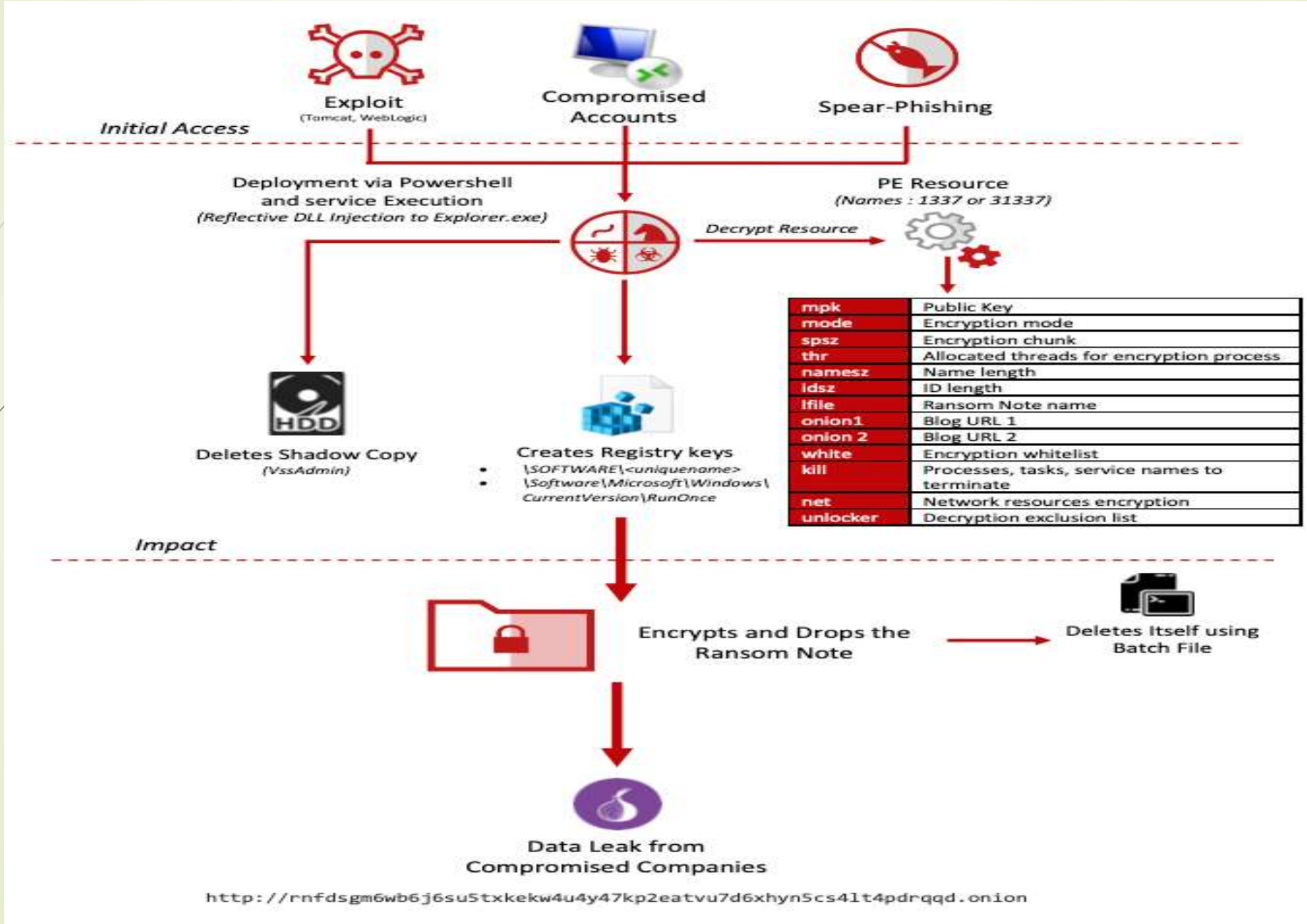
Вирус-шифровальщик Netwalker

Netwalker — это быстро набирающая масштабы программа-вымогатель, созданная в 2019 году группой киберпреступников, известной как Circus Spider. На первый взгляд Netwalker действует, как и большинство других разновидностей программ-вымогателей: проникает в систему через фишинговые письма, извлекает и шифрует конфиденциальные данные, а затем удерживает их для получения выкупа.

Сферы, атакуемые Netwalker

- образование
- здравоохранение
- производство;
- управление бизнесом;
- управление потребительским опытом и качеством обслуживания;
- электромобили и решения для накопления электричества;

Схема пути атаки Netwalker



Советы по защите от программы-вымогателя Netwalker

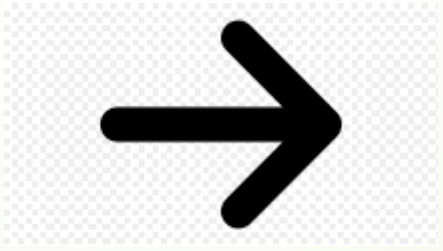
- Выполнять резервное копирование важных данных на локальные хранилища данных;
- Убедиться, что копии критически важных данных хранятся в облаке, на внешнем жестком диске или устройстве хранения;
- Защитить свои резервные копии и убедиться, что данные невозможно изменить или удалить из системы, в которой они хранятся;
- Установить и регулярно обновлять антивирусное программное обеспечение на всех компьютерах;
- Использовать только безопасные сети и избегайте общедоступных сетей Wi-Fi. По возможности используйте VPN;
- Использовать двухфакторную аутентификацию с надежными паролями;
- Регулярно обновлять компьютеры, устройства и приложения.

Развитие киберпреступлений

- *Киберпреступность - это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей.*

Киберпреступность растет более быстрыми темпами, чем все другие виды преступности.

- *Число пользователей Интернета составляло:*
  в 2000 г - 400 млн чел., то в настоящее время в мире насчитывается более 3,2 млрд.


- *Так, уровень киберпреступности повысился с 24% в 2014 г. до 32% в 2016 г., заняв вторую позицию среди видов экономической преступности в мире*

Как поменялись хакеры

Если первоначально это были люди, обладавшие знаниями, умениями, направлявшие свои действия не столько на противозаконные цели, сколько на поиск нового,
То в настоящее время за преступными действиями стоит криминальный бизнес.

иметь гражданство одной страны

находиться на территории другой

работать через сервер, расположенный в третьей стране

Продолжительность самих атак при этом варьируется в достаточно большом временном интервале:

от нескольких секунд до суток и месяцев.

Малый и средний бизнес

Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса в следствии :

- малого бюджета
- отсутствия квалифицированных кадров
- пробелов в познаниях сотрудников о кибербезопасности

Для больших компаний, защита конфиденциальной информации, интеллектуальной собственности имеет принципиально важное значение для успешного ведения бизнеса и требует разработки комплексной стратегии безопасности, исходя из целей деятельности компании.

Интернет-банкинг

Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений.

1. Расширение применения электронных технологий увеличило возможности киберпреступников
2. Дистанционное банковское обслуживание требует комплексной защиты от фишинга и троянов
3. Использование банками устаревших технологий, не способных противостоять преступникам

Борьба с кибер-преступностью

Для комплексного противодействия киберпреступности необходимы:

– гармонизация уголовного законодательства о киберпреступности на международном уровне;

- разработка на международном уровне и имплементация в национальное законодательство процессуальных стандартов
- отлаженное сотрудничество правоохранительных органов
- механизм решения юридических вопросов в киберпространстве.

На государственном и уровне частных предприятий необходимо активно заниматься профилактической, просветительской деятельностью.

- Повышение компетенции в сфере компьютерных технологий
- Компьютерная грамотность населения
- пользователям необходимо научиться быть менее беспечными

Вывод

Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений.

Необходимость защиты от киберпреступников очевидна. Желательно, чтобы на уровне государства решались проблемы борьбы с киберпреступлениями, а повсеместно проводить работу по разъяснению ограждения от киберпреступников.

Наша безопасность в наших руках! Мы за безопасность использования информационного пространства.

Спасибо за внимание!