Санкт-Петербургское государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный институт психологии и социальной работы»

Социально-психологические риски для подростков в киберпространстве

Автор доклада:
Ермин Дмитрий Алексеевич
E-mail: ermin101@mail.ru

Киберпространство – это:

- Генератор возможностей;
- Источник угроз;
- Еще один театр военных действий.

Информация – все то, что может быть представлено в символах конечного (например, бинарного) алфавита.

Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Угрозы безопасности

Для государства

- Информационные войны
- Кибер атаки
- Кибер шпионаж
- Кибер преступность
- Кибер терроризм
- Распространение секретных сведений

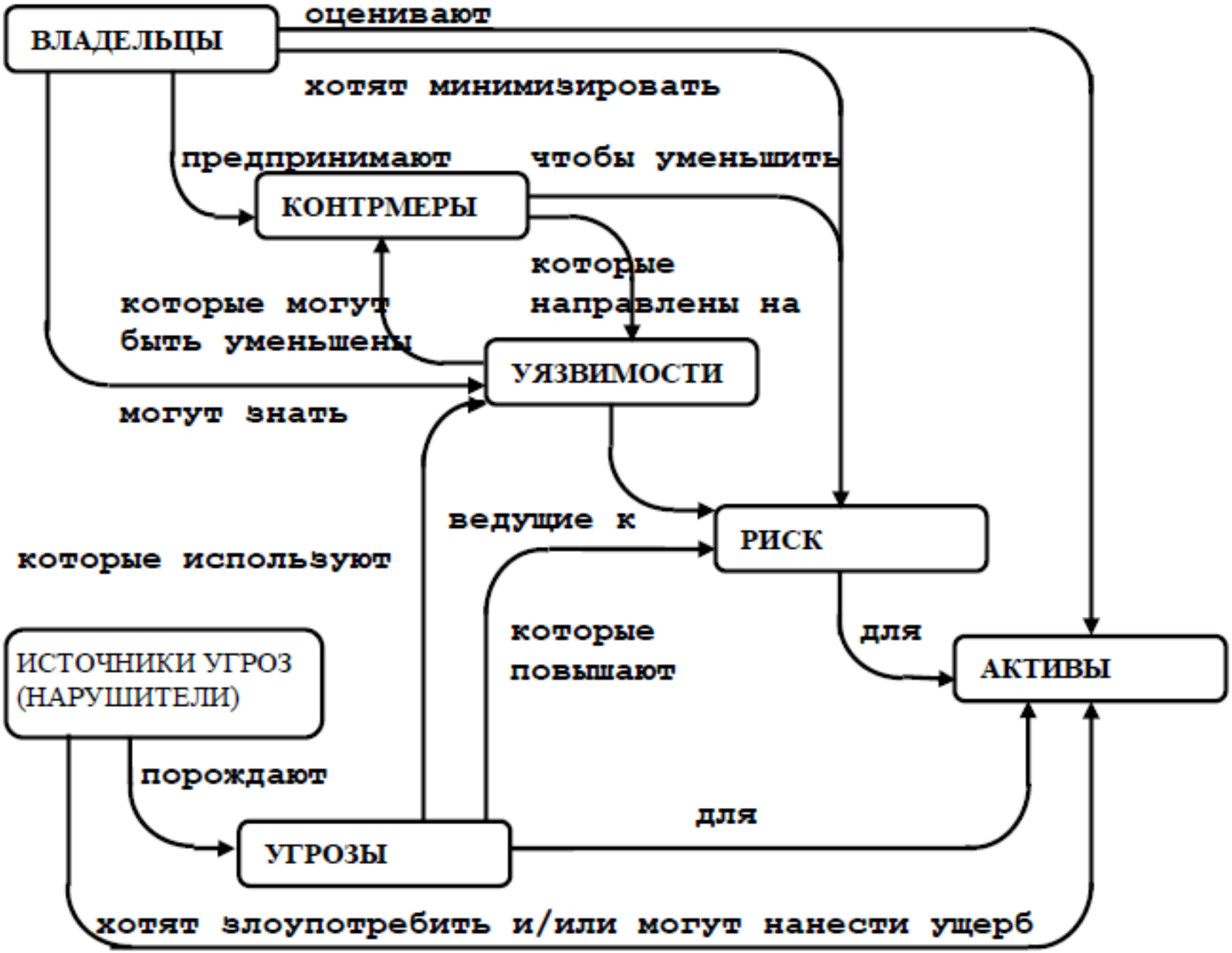
Для бизнеса

- Разглашение коммерческой тайны
- Утечка данных
- Несанкционированный доступ

Для граждан

- Кибер слежка
- Мошенничество
- Фишинг
- Вишинг
- Фарминг

Общая схема процесса обеспечения безопасности



Риски направлены на:

- **Деньги** (мошенники, платные подписки, шантаж);
- **Устройства** (вирусы, черви, рекламное ПО, шпионское ПО, боты и криптоджекинг);
- **Личность** (кибербуллинг, фейковые новости, вбросы, ментальные вирусы, клиповое мышление, привычка к соцсетям, деструктивные сообщества);
- **Общество** (снижение уровня доверия, смещение ценностей, внедрение идеологии, снижение ответственности).

Фишинг или социальная инженерия – атаки на пользователей для получения конфиденциальной информации (например, паролей от кредитных карт).
Фишинг обычно представляет собой рассылку писем, похожих на сообщения от авторитетных источников, или рекламы.
Вишинг (англ. vishing) — от слов «voice» и «phishing», «голосовой фишинг», то есть попытка мошенников обманом выведать у жертвы какие-то конфиденциальные сведения по телефону.

Фарминг – скрытая переадресация пользователей на поддельные сайты для последующей установки вредоносного ПО или похищения конфиденциальных данных.
Спуфинг – создание клонов доменов или программ, которые ничего не подозревающие пользователи принимают за оригинальные и вводят на них свои данные.
Криптоджекинг – воровство ресурсов устройства для добычи криптовалюты.

Термин «**Вредоносное ПО**» (Malware - от англ. «malicious software») используется для описания любой вредоносной программы на компьютере или мобильном устройстве.

Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера.

1. Вирусы (Virus)

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере.

Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях.

2. Черви (Worm)

Червям для распространения **не требуется вмешательство человека**: они заражают один компьютер, а затем через компьютерные сети распространяются на другие ПК без участия их владельцев.

Используя уязвимости сети, черви могут отправлять тысячи своих копий и заражать все новые системы. Черви «съедают» системные ресурсы, снижая производительность компьютера, большинство из них содержит вредоносные составляющие.

3. Рекламное ПО (Adware)

Среди разновидностей Adware - всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО.

Поскольку Adware устанавливается с согласия пользователя, такие программы нельзя назвать вредоносными: обычно они идентифицируются как «потенциально нежелательные программы».

4. Шпионское ПО (Spyware и Keylogger)

Собирает информацию (например, нажатия клавиш на клавиатуре ПК, отслеживает, какие сайты посещает пользователь и даже перехватывает регистрационные данные), которая затем отправляется третьим лицам, как правило, киберпреступникам.

Оно также может изменять определенные параметры защиты на компьютере или препятствовать сетевым соединениям.

5. Программы-вымогатели (Winlock)

Программы-вымогатели заражают ПК, затем шифруют конфиденциальные данные (личные документы или фотографии) и требуют выкуп за их расшифровку.

Если пользователь отказывается платить, данные удаляются.

Некоторые типы программ могут полностью заблокировать доступ к ПК.

Они могут выдавать свои действия за работу правоохранительных органов и обвинять в каких-либо противоправных поступках.

6. Боты (Zombie)

Предназначены для автоматического выполнения определенных операций.

Могут использоваться для легитимных целей, но злоумышленники приспособили их для себя.

Бот-сеть может использоваться для удаленного управления взломанными машинами: кражи конфиденциальных данных, слежки за действиями жертвы, распространения спама или DDoS-атак сайтов.

7. Руткиты (Rootkit)

Позволяют получать удаленный доступ к компьютеру и управлять им. Проникнув в компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить личные данные или установить другие вредоносные программы. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.

8. Троянские программы (Trojan)

Эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

9. Баги (Bug)

Баги - ошибки в фрагментах программного кода, допущенные программистом. Они могут иметь пагубные последствия для компьютера, такие как остановка, сбой или снижение производительности.

Профилактические мероприятия

- Использование лицензионного ПО;
- Использование только своих флешек;
- Игнорирование неизвестных программ;
- Избегание перехода по ссылкам в сообщениях;
- Ограничение доступа к вашему ПК;
- Создание нескольких пользователей при работе на одном ПК;
- Использование песочницы и виртуальных машин;
- Регулярное обновление программ;
- Использование нескольких антивирусных программ.

Литература

Кларк Р. Третья мировая война: какой она будет?: высокие технологии на службе милитаризма / Cyber War: the Next Threat to National Security and What To Do About It. - СПб.: Питер, 2011. - 336 с.

Ашманов И. Цифровая Гигиена - СПб.: Питер, 2022. - 400 с.