Введение

Причины инструктажа:

- ✔ увеличение количества нарушений информационной безопасности работниками;
- ✔ легкомыслие работников в вопросах информационной безопасности;
- ✔ массовые заражения компьютеров крупных компаний вирусами-шифровальщиками (такими как WannaCry);
- ✔ повышение эффективности вирусных компаний.

Крупные жертвы вирусов ExPetry и WannaCry:

- ✔ МВД России;
- ✔ Мегафон;
- ✔ Роснефть;
- ✔ Башнефть;
- ✔ Банк «Хоум Кредит» и др.

1.1. Основные угрозы

✔ **Источниками вирусного заражения являются**:

- фишинговые рассылки (письма-уловки) на электронные адреса работников;
- посещение работниками вредоносных сайтов;
- использование сторонних, а не выданных, USB-накопителей (флешек) (в т.ч. личных или подрядчиков);
- подключение к рабочему АРМ (в нарушение Инструкции по ИБ) личных смартфонов.

✔ **К компрометации учетных данных ведут** следующие действия работников:

- умышленная передача коллегам логинов-паролей;
- использование стандартных паролей (1qaz2wsx, 123456, имена, фамилии, номера телефонов, даты рождения и т.д.);
- подбор логинов-паролей вредоносным программным обеспечением.

1.2. Электронная почта

- ✔ **Электронная почта** – один из самых эффективных каналов доставки вредоносного программного обеспечения.
- ✔ **Признаки потенциально опасных писем**:
  - получение письма от неизвестного адресата (злоумышленники часто выдают себя за представителей операторов связи, банков, коммунальных служб);
  - вложения от неизвестных адресатов в зашифрованном архиве с указанием пароля в тексте письма;
  - несоответствие предполагаемого содержимого и типа файла (например, счет-фактура с расширением EXE, CMD, JS или VBS);
  - указание в тексте письма ссылки для скачивания документа;
  - использование существующих адресов корпоративной электронной почты работников _____ в качестве отправителя спама.

1.2. Электронная почта

Первый пример фишингового письма

Адрес ссылки на скачивание и реальный (подсвеченный) адрес сайта не соответствуют друг другу.

Второй пример фишингового письма

К письму прикладывается архив с вирусом (или ссылка на скачивание), который может выглядеть как скан (pdf) или документ Word/Excel, но имеет расширение исполняемого файла (exe, com, scr и др.).

1.2. Электронная почта

Опасность фишинговых рассылок в том, что злоумышленниками автоматизировано генерируется огромное количество вариаций вредоносного программного обеспечения и антивирусные средства запаздывают на 1-2 дня. Этого обычно достаточно для достижения высокой эффективности атак.

Реальный собеседник скорее всего свяжется для подтверждения получения.

1.2. Электронная почта

Распространенное заблуждение сотрудников – «моя учетная запись и информация, имеющаяся на моем компьютере, никому не интересны, требование сложности паролей и их периодическая смена не обоснованы».

Персональная учетная запись – цифровое удостоверение личности пользователя. Учетная запись определяет к каким информационным ресурсам пользователь имеет доступ и какие действия с ними может выполнять.

Имеющаяся на Вашем компьютере информация, которую Вы можете считать не интересной и общедоступной, может представлять огромный интерес для злоумышленников.

Оборотной стороной наличия прав является ответственность пользователя за их применение.

Мало кого обрадует, если выяснится, что массив документов подразделения за несколько лет был уничтожен от имени его учетной записи или в системе документооборота от его имени создан или согласован документ, несущий серьезные финансовые или репутационные риски.

1.3. Защита учетных данных

Кто может воспользоваться учетными данными:

- ✔ недобросовестные коллеги;
- ✔ вредоносное программное обеспечение;
- ✔ злоумышленники.

Меры защиты:

- ✔ передавать персональные учетные записи коллегам только при острой необходимости и по согласованию с руководителем структурного подразделения;
- ✔ использовать сложные пароли, содержащие спецсимволы, цифры, буквы в верхних и нижних регистрах, а также периодически менять их.

1.4. Интернет

Ограничение доступа к сети Интернет не прихоть, а необходимая мера защиты.

Обеспечение безопасности крупных и популярных сайтов задача сложная и дорогостоящая.

Поэтому большинство развлекательных ресурсов получают доход от рекламы и содержат множество ссылок на сторонние ресурсы, нередко вредоносные. Отсутствие внимания к безопасности приводит ко взломам и дальнейшему распространению вредоносного ПО.

Потенциально опасные ресурсы, **запрещенные** к посещению на рабочем месте:

- социальные сети;
- файлообменные сервисы и облачные хранилища;
- неофициальные сайты по распространению ПО и драйверов;
- сайты развлечений (демотиваторы, котики, приколы и т.д.).