ЗАДАНИЯ ПО ДИСЦИПЛИНЕ
«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

Задания оформляются в виде электронного отчета формата MS Word или MS PowerPoint со следующим содержанием:

- ✓ титульный лист с данными студента;
- ✓ описание задания;
- ✓ пошаговое описание выполнения работы со скриншотами и личными поясняющими комментариями;
- ✓ список использованных программ с указанием их официального и проверенного URL-адреса дистрибутива;
- ✓ список использованных статей и материалов с указанием URL-адресов.

К защите допускаются работы при наличии:

- ✓ оформленного электронного отчета, пересланного преподавателю;
- ✓ установленного, запущенного и настроенного программного обеспечения для демонстрации проделанной работы и защиты отчета.

№ практ. работы	Задание практической работы	Основное программное обеспечение	Примечание
1	Сделать персональную портативную версию безопасного браузера с установленными расширениями безопасности. Организовать безопасную связь через защищенный чат	Mozilla Firefox (portable) + расширения ->	uBlock Origin, HTTPS-Everywhere, Ghostery, Flashblock, LastPass, Unhide Passwords, Mailvelope, Mega, Cryptodog, Frigate
2.1	Освоить безопасное хранение и использование паролей	Mozilla Firefox (portable) + LastPass	Создание аккаунта, сохранение и использование паролей
2.2	Освоить работу с криптозащищенными файловыми хранилищами	Mozilla Firefox (portable) + Mega	Создание аккаунта, добавление контактов, работа с данными хранилища
2.3	Изучить средства обеспечения конфиденциальности данных для обычных облачных систем	CryptSync, EncFS MP, AxCrypt	Установка и тестовое использование указанных программ
3.1	Изучить возможности защищенного онлайн-общения	Telegram, qTox, Bitmessage, Pidgin + OTR	Регистрация, обмен данными, сохранение и перенос данных аккаунта
3.2	OpenPGP для использования в безопасной переписке	gpg4usb, Telegram	Создание персональной пары криптоключей, подписание и зашифровывание сообщений, проверка подписей и расшифровка сообщений

3.3	Сделать персональную сборку почтового клиента с установленными расширениями безопасности и конфиденциальности	Mozilla Thunderbird с Enigmail (portable) + gpg4win (portable)	Отправка и получение зашифрованных и подписанных сообщений
4.1	Безопасное удаление и восстановление данных на физических носителях	Recuva Hardwipe	Восстановление удаленных файлов Удаление файлов и папок без возможности восстановления
4.2	Безопасное хранение данных на физических носителях	TrueCrypt	Создание и использование защищенного файлового контейнера Удаление метаданных из документов и медиаконтента
4.3	Стенография (скрытие и подписывание) данных с помощью изображения, звука и видео	OpenPuff	Скрытие и извлечение текстовой информации с помощью графических, звуковых и видеофайлов
4.4	Защита данных в мобильном устройстве	Android: Orbot, Orfox, K-9 Mail + APG, Telegram, Freelab Messenger + OpenKeychain, Signal, Antox iOS: oPenGP, iPGMail, SJ IM, Telegram, Signal	VPN, безопасный серфинг, работа с ключами OpenPGP, криптопочта, крипточат
5	Поиск и защита от вредоносного программного обеспечения и программ-шпионов	Autoruns, Process Explorer, TCPView, CCleaner, AdwCleaner	Поиск и удаление ненужных и/или вредоносных файлов в автозапуске, процессах. Проверка сетевых соединений на несанкционированный трафик. Поиск и удаление шпионских модулей и программ
6	Безопасные открытые операционные системы	VirtualBox + Linux Mint (live)	Установка в виртуальной машине безопасной ОС, настройка браузера, почтового клиента и мессенджера на безопасное взаимодействие по сети
7	Информационная безопасность и аудит программного обеспечения	InqSoft Windows Scanner, PE Explorer, UPXN	Разработка простейшей визуальной программы с контролем доступа и конфиденциальной информацией. Реверс-инжиниринг программы. Защита программы динамической компрессией
8	Информационная безопасность данных в сети. Системы информационной безопасности	Wireshark, Lizard Network Scanner, LanSpy	Сканирование локальной сети на наличие уязвимостей данных