# Первая таблица

|  |  |  |
| --- | --- | --- |
| № | Пример охраняемой законом информации | Каким законом она охраняется |
| 1 | Государственная тайна | Защищается законом «О государственной тайне» № 5485-1 |
| 2 | Личная и семейная тайна | Охраняется Конституцией РФ, статья 23 |
| 3 | Врачебная тайна | Охраняется законом «Об основах охраны здоровья граждан в Российской Федерации» № 323-Ф3 |
| 4 | Коммерческая тайна | Охраняется федеральным законом «О коммерческой тайне» №98-Ф3 |
| 5 | Профессиональная тайна | Охраняется законом «Об информации, информационных технологиях и о защите информации» № 149-Ф3 |
| 6 | Тайна следствия и судопроизводства | Охраняется уголовно-процессуальным кодексом, статья 161 № 174-Ф3 |
| 7 | Аудиторская тайна | Охраняется законом «Об аудиторской деятельности» №307-Ф3 |

# Вторая таблица

|  |  |  |
| --- | --- | --- |
| № | Пример вредоносного ПО с описанием функционала | Признаки из ст.273 |
| 1 | Michelangelo – вирус 1992 года. Работал в загрузочной записи BIOS. Каждое 6 марта он перезаписывал первые 100 секторов жесткого диска на нули. | Несанкционированное уничтожение или модификация информации |
| 2 | Melissa – макровирус 1999 года. Заражал файлы MS Word и распространял себя через рассылку всем из адресной книги электронной почты. Так же пересылал другие файлы | Копирование компьютерной информации |
| 3 | Haxdoor – вирус 2005 года. Троян, предназначенный для кражи персональных данных. Использовал руткиты на уровне ядра и мог деактивировать антивирусное ПО, удалять данные на дисках и завершать работу ОС | Несанкционированное уничтожение и блокировка информации. Нейтрализация средств защиты компьютерной информации |
| 4 | Virus.Win9x.CIH – вирус 1998 года. При запуске внедряет свой код в память ОС и начинает перехватывать запуск .exe файлов, записывая в них свою копию. Уничтожает данные на жестких дисках, а в некоторых случаях на микросхемах BIOS | Несанкционированное уничтожение информации |
| 5 | Sasser – вирус 2004 года. Распространялся через уязвимость в одной из служб Microsoft. Создавал FTP сервер, затем создавал файл с IP адресом компьютера, который пытался | Несанкционированная блокировка информации |
| 6 | CryptoLocker – вирус 2013 года. Троян распространялся через зараженные файлы в электронной почте. После распространения, троян шифровал файлы офисных пакетов и выводил на экран сообщение о блокировке файлов. | Несанкционированная блокировка информации |
| 7 | WannaCry – вирус 2017 года. Использовал для распространения уязвимость в ОС Windows. После распространения шифровал информацию на ПК. | Несанкционированная блокировка информации |

# Три примера вредоносной информации, не являющейся ПО

1. Некоторый т.н. «лайфхаки» или шутки. К примеру, если положить шарик из фольги в микроволновку, то он станет гладким. Но на деле вызываются электрические искры, которые приводят к поломке техники.
2. Фейки, дающие заведомо ложную информацию. Яркий пример – распространение фейка о принципе действия прививки от COVID-19. В период активной вакцинации огромное количество людей считало, что государство хочет их чипировать или специально заразить. Следовательно люди, верящие в это, не вакцинировались и подвергали риску других людей, а также провоцировали нагрузку на медицинские учреждения.
3. Фейк об увольнении финансового директора французской компании Vinci. Из-за данного фейка акции упали на 20% и принесли ущерб в размере 7 миллиардов евро.