увеличивается до 630 кг/м$^3$ , повышение температуры в этих составах приводит к снижению плотности до 450 кг/м$^3$ и увеличению пористости до 78 %. Очевидно, это связано с взаимодействием известняка со щелочью, что и приводит к снижению активности вспенивания.

Изготовление пеностекла по гидратному механизму, где в качестве основного сырьевого материала применялось битое стело в смеси с гидроксидом натрия, с целью увеличения пористости вводился карбонатный порообразователь – известняк. Однако использование этой добавки оказалось нерационально, так как готовые образцы получались недостаточно пористыми из-за того, что происходила химическая реакция известняка с гидроксидом натрия, в результате которой замедлял процесс газовыделения.

**Список использованной литературы**

1. Сеник Н.А. Составы и технология получения гранулированного пеностеклокристаллического материала на основе композиций диатомита с гидроксидом натрия: дис…. канд. техн. наук. Томск, 2013.

2. Маневич В.Е., Никифоров Е.А., Мешков А.В. [и др.]. Высокоэффективный теплоизоляционный материал на основе диатомового сырья // Строительные материалы. 2012. № 11. С. 18 – 22

3 Особенности синтеза пеностекла на основе диатомитового сырья / Б.М. Гольцман, Е.А. Яценко, В.С. Геращенко, Н.Ю. Комунжиева // Экология промышленного производства. 2018. № 4. С. 23 – 25.

4. Гольцман Б.М., Геращенко В.С., Комунжиева Н.Ю., Яценко Л.А. Исследование возможности использования мела как интенсификатора вспенивания при синтезе пеностекольных материалов// Известия вузов. 2019. № 3. С.82-86

## ВРЕДОНОСНЫЕ ПРОГРАММЫ КАК ОПАСНОСТЬ ОВД.

DOI: 10.31618/ESU.2413-9335.2020.1.72.619

***Смирнов Виталий Михайлович,***
*к.т.н*
*Московский университет МВД России им. В.Я. Кикотя*
***Киселёв Сергей Александрович***
*Московский университет МВД России им. В.Я. Кикотя*

**АННОТАЦИЯ**
В статье раскрываются основные виды вредоносных ПО и методы борьбы с ними.
**ANNOTATION**
The article describes the main types of malware and methods for dealing with them.
**Ключевые слова***:* Компьютер, программа, нарушение, вирус, Программное Обеспечение, вред.
**Keywords**: computer, program, violation, virus, software, harm.

Ни для кого не секрет, что в наше время, пожалуй, большинство пользователей ощущали на себе всю отрицательную сторону развития информационных технологий, конкретно – вредоносных программ. Сейчас, когда большая часть информации хранится на электронных носителях, особенно важно повышать уровень безопасности и сохранности этой информации от влияния всевозможных угроз. Данное явление не обошло стороной и ОВД, ведь в распоряжении этой системы федеральных органов находятся данные о всех гражданах Российской Федерации и совершённых преступлениях. При завладении такими данными, преступники окажутся на порядок опаснее, чего допустить нельзя.

В сложившихся условиях особую актуальность приобретает вопрос борьбы с вредоносными программами.

Вредоносная программа – это компьютерная программа, предназначенная для причинения ущерба ПК, независимо от вида данной программы.

Идея создания вредоносных ПО возникла в 1946 году. Именно тогда американец Джон фон Нэйманн создал теорию о самовоспроизводящихся программах. Данное исследование явилось отправной точкой в мире компьютерных вирусов. Спустя некоторое время, в 1959 году, его соотечественником, Л.С. Пенроузом была опубликована статья о самовоспроизводящихся механических структурах, в которой речь шла о двухмерных структурах, способных к активации, размножению и захвату.

С тех пор в нашем мире много чего изменилось, появились миллионы новых вредоносных программ, увеличилась и их опасность для общества. В связи с этим, в Уголовный Кодекс Российской Федерации были внесены следующие статьи:

- Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

- Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

•Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Безусловно, как это и говорилось ранее, в наше время существует множество разнообразных вредоносных программ, но их объединяют одинаковые цели:

•Распространение вредоносного ПО

•Нарушение работы ПК

•Сообщение пользователю заведомо ложной информации о своих действиях в системе

•Сокрытие своих действий от антивирусных программ

Также у большинства таких программ действует одинаковая последовательность действий, которая выглядит следующим образом:

1.Заражение ПК

2.Активация вредоносной программы

3.Поиск файлов для заражения вредоносной программой

4.Заражение выбранных файлов вредоносной программой

Такие программы могут нанести существенный вред деятельности ОВД. Они имеют множество разновидностей, основные из них:

•Компьютерные вирусы – вредоносное ПО, способное внедряться в код других программ, повреждать данные пользователя, изменять содержимое файлов и распространяться.

•Сетевые черви – вредоносное ПО, способное к самостоятельному распространению через локальные, либо глобальные (интернет) сети. По функционалу схожи с вирусами. Целью сетевых червей является заражение файлов для дальнейшего распространения на другие компьютеры.

•Троянские программы – вредоносное ПО, способное к выполнению задач, специально определённых правонарушителем, таких как нарушение работы компьютера, кража данных пользователя, удаление данных пользователя и др.

Пути проникновения программ, вызывающих сбои в работе компьютера и причиняющих ущерб пользователю: съёмные диски; флеш-накопители; файлы, загруженные из сети Интернет; электронная почта; пиратское ПО.

Наравне с вредоносными программами развиваются и методы защиты от них. Наиболее эффективным средством борьбы с вирусами принято считать антивирус.

Антивирус – это программа, созданная для борьбы с нежелательными программами, вызывающими нарушения в работе ПК, заражение и повреждение данных пользователя.

В большинстве случаев, в антивирусах заложено два подхода к обнаружению заражённого файла, либо самого вредоносного ПО – сигнатурный и проактивный. Первый из этих способов осуществляет поиск нежелательных программ по характерным для них чертам, путём сравнения известных признаков вируса с признаками, имеющимися у файла. Проактивный метод обнаружения вредоносных ПО заключается в анализе поведения файла при его работе.

Помимо антивирусных программ, также есть такой способ борьбы с вредоносным ПО, как профилактические меры. Они заключаются в регулярной чистке компьютера от неиспользуемых и незнакомых пользователю программ.

Говоря о борьбе с вредоносными программами в ОВД, нельзя не упомянуть тот факт, что сейчас действует программа перехода с операционной системы Windows на российскую Astra Linux. Согласна плану, доля отечественной операционной системы в таких органах государственной власти, как МВД, ФСО, ФСИН и ФСБ в 2020 году должна составлять не менее 80%. Объясняется это тем, что ОС Linux гораздо безопаснее, т.е. имеет значительно меньшее количество нежелательных программ, угрожающих целостности и конфиденциальности данных пользователя.

Таким образом, можно утверждать, что вредоносные программы действительно способны нанести серьёзный ущерб ОВД в виде повреждений данных, похищении важной информации и нарушении работы ПК в целом. Все перечисленные действия направлены на замедление работы правоохранительных органов. Способы борьбы с ними постоянно должны совершенствоваться, чтобы дать достойный отпор преступникам.

**Библиографический список:**

История возникновения вредоносных ПО – https://studwood.ru/1699944/informatika/istoriya_vozniknoveniya_vredonosnyh

Компьютерные вирусы: Происхождение – https://www.nkj.ru/archive/articles/7889/

Классификация вредоносных программ – https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/

Пути проникновения вирусов в компьютер – //vuzlit.ru/1035575/puti_proniknoveniya_virusov_kompyuter_mehanizm_raspredeleniya_virusnyh_programm

Статья «Переход с Windows на Astra Linux» – https://habr.com/ru/news/t/410097/

Уголовный Кодекс Российской Федерации