Таким образом можно сделать вывод, что кибербезопасность играет ключевую роль в современном информационном обществе, и ее значимость будет продолжать расти по мере развития цифровых технологий. Понимание основных тем и направлений кибербезопасности поможет эффективно защитить информацию и данные от киберугроз. Важно осознавать угрозы киберпреступности и принимать необходимые меры для обеспечения безопасности в цифровом мире.

Литература

1. Лутонин А. С. Введение в кибербезопастность. : Учебное пособие для студентов вузов. [Текст] / А.С. Лутонин – Санкт-Петербург, 2022. – 63с.

2. Как защитится от кибератак. // [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-zashchititsya-ot-kiberatak/ Дата доступа: 25.03.2024.

ВРЕДОНОСНЫЕ ПРОГРАММЫ И ИХ КЛАССИФИКАЦИЯ. ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ И ДРУГИХ ВРЕДОНОСНЫХ ПРОГРАММ

Гутырчик К.А., Котович Е.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В нынешнее время, в эпоху цифровых технологий и программирования пользователи подвергаются высоким рискам, связанным с угрозой их компьютерной и персональной безопасности, а также утечками пользовательских данных в сети Интернет. Данные процессы в большинстве своих случаев возникают в связи с нахождением вредоносных или же вирусных программ и плагинов на персональном устройстве пользователя. Вредоносные программы являются одним из главных инструментов злоумышленников для нанесения ущерба за получение пользовательской информации и данных, а также внедрения своих вредоносных материалов. В данной сфере, важным аспектом является понимание классификации, видов, а также методов заражения таковыми программами. [3]

Современным обществом принято выделять следующие типы вредоносных программ:

1. Файловые вирусы — это программы, способствующие заражению исполняемых файлов, добавляя в них свой код. Этот процесс позволяет им передаваться на другие компьютеры через уже зараженные файлы. [4]

2. Макровирусы — представляют собой разновидность вредоносных программ, которые используют макросы в приложениях. Они внедряются в документы и могут выполнить недоброжелательные действия при открытии таких файлов. Макровирусы берут контроль над макросами и могут заражать другие файлы, которые используют эти макросы. [6]

3. Кибершпионажные программы — это вредоносные программы, созданные для незаконного сбора информации о деятельности пользователей. Они имеют способность перенимать пароли, отслеживать нажатия клавиш и даже могут получать доступ к веб-камере пользователя без его согласия. [1]

4. Рекламные программы (adware) — это программы, которые показывают рекламу пользователю без его согласия. Они могут отобразить нежелательные всплывающие окна, перенаправить пользователя на рекламные сайты или внедриться в браузеры для отображения рекламных баннеров. [2]

5. Руткиты — это тип вредоносных программ, которые скрывают свои действия, модифицируя операционную систему. Они могут незаметно перехватывать данные, маскировать процессы и обеспечивать злоумышленнику полный контроль над зараженной системой. [5]

6. Троянские программы — представляют собой вредоносные приложения, которые маскируются под полезные программы с целью несанкционированного доступа к компьютеру или к получению конфиденциальной информации. Они способны заразить систему через множество путей, такие как электронная почта и веб-сайты. [7]

7. Черви — это самостоятельные вирусы, способные распространяться без участия пользователя. Они используют различные уязвимости в системе или сети для своего распространения и могут создавать огромные ботнеты. [9]

8. Ботнеты — это сети зараженных компьютеров, которые находятся под контролем злоумышленников. Эти компьютеры могут быть использованы для различных вредоносных действий, включая отправку спама и проведение DDoS-атак. [8]

9. Шпионское ПО: Шпионские программы тайно отслеживают и собирают информацию о действиях пользователя, например о его привычках просмотра веб-страниц, нажатиях клавиш или личных данных, без его согласия. Полученные данные затем могут быть переданы злоумышленникам для использования в недобросовестных целях, таких как кража личной информации или направленная реклама.

Распространение вредоносных программ основывается на использовании разнообразных способов передачи, включая как технические уязвимости, так и человеческую доверчивость.

Один из самых распространенных методов — это использование электронной почты: фишинговые сообщения, содержащие вредоносные приложения или ссылки на зараженные веб-сайты, являются одним из наиболее широко распространенных способов распространения вредоносных программ. Киберпреступники используют тактику социальной инженерии, чтобы обманом заставить пользователей невольно выполнить вложения с вредоносным ПО или посетить скомпрометированные веб-сайты.

Злоумышленники проникают в законные веб-сайты, внедряя вредоносный код или используя уязвимости в программном обеспечении веб-приложений. Пользователи, посещающие такие скомпрометированные сайты, могут случайно загрузить вредоносное программное обеспечение на свои системы, тем самым способствуя его дальнейшему распространению

Использование сетей: Вредоносное ПО распространяется по сети путем использования уязвимостей в сетевых службах или программном обеспечении. Например, черви используют такие уязвимости для автоматического распространения по взаимосвязанным системам, взламывая слабые системы с недостаточной настройкой сетевой безопасности.

Съемные носители: USB-накопители и другие съемные устройства хранения данных служат каналами для передачи вредоносного ПО. Обычный пользователь при подключении USB-накопителя даже и не заметит, как его устройство заразилось каким-нибудь вредоносным компонентом, так как они распространяются по хост-системе и другим устройства, подключённым к исходному.

Литература

1. Иванов А.Г. Компьютерные вирусы: распространение и методы борьбы. Москва: Издательство "БХВ-Петербург", 2016.
2. Козлов В.Д. Троянские программы: механизмы работы и защита. Москва: Издательство "БХВ-Петербург", 2020.
3. Назимов А.Ф. Вирусы и антивирусы. Москва: Издательство "Эксмо", 2015.
4. Петров В.С. Кибершпионаж: актуальные проблемы и тенденции. Москва: Издательство "Лори", 2018.
5. Семенова Е.М. Информационная безопасность и защита от вредоносных программ. Москва: Издательство "Проспект", 2017.
6. Сидоров П.Н. Вредоносные программы: обзор и анализ. Москва: Издательство "Питер", 2019.
7. "Types of Malware: Explained". Security Intelligence.[Электронный ресурс]. — Режим доступа: https://www.ibm.com/security/intelligence/types-of-malware- — Дата доступа: 07.04.2024

8. "Understanding Adware". Norton. [Электронный ресурс]. — Режим доступа: https://us.norton.com/internetsecurity-malware-understanding-adware.html— Дата доступа: 07.04.2024

9. "What are Botnets?". US-CERT. [Электронный ресурс]. — Режим доступа:https://www.us-cert.gov/ncas/tips/ST04-001— Дата доступа: 07.04.2024

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ТАМОЖЕННОМ ДЕЛЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Гутырчик К.А., Котович Е.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В эру активного развития технологий, автоматизации процессов и совершенствования программного обеспечения использование информационных источников и ресурсов является опорной базой всех отраслей жизнедеятельности человека, в том числе таможенных органов. В данном реферате мы рассмотрим основные аспекты использования компьютерных технологий в таможенном деле Беларуси. [2]

Основные аспекты использования компьютерных технологий в таможенном деле Беларуси:

1. Автоматизация таможенных процедур. Система автоматизации таможенных процедур ускоряет и упрощает работу таможенного оформления. В Беларуси внедрены современные информационные системы, такие как "Единое окно" и "АСЭНДА", которые позволяют эффективно управлять таможенными операциями. [3]

2. Электронная декларация и таможенное оформление благоприятно повлияли на снижение уровня бюрократии, а также облегчили и ускорили работу таможенников. Введение электронной декларации также способствует уменьшению вероятности ошибок и мошенничества.

3. Использование баз данных и аналитических инструментов. Сбор и анализ данных о таможенных операциях позволяет выявлять тенденции и аномалии, оптимизировать процессы и принимать обоснованные управленческие решения. Базы данных также используются для хранения информации о таможенных пошлинах, тарифах и других регулирующих параметрах. [1]

4. Электронный мониторинг грузов. В последние годы таможенными органами Республики Беларусь применяется электронное пломбирование транспортных средств, перемещающих коммерческие товары. В связи с данной процедурой был введен мониторинг, отслеживающий передвижение