# ОЦЕНКА РАЗНООБРАЗИЯ УСТАНОВОЧНЫХ СРЕДСТВ НА РЫНКЕ: АНАЛИЗ ДОСТУПНЫХ МЕТОДОВ ВЗАИМОДЕЙСТВИЯ С ПАРАМЕТРАМИ СОГЛАСИЙ

*Бердник Л. А.[1], студент гр.153502, Михалевич М. П.[2], студент гр.153504, Рогов М.Г.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

**Аннотация.** Исследование рассматривает разнообразие установочных средств на рынке, фокусируясь на методах получения согласия пользователя с целью установки нежелательного ПО. Распространенная практика использования "нежелательных галочек" приводит к загрузке ненужных программ, негативно влияя на пользователей и подрывая доверие к разработчикам. В работе анализируются различные методы взаимодействия с параметрами согласий, применяемые в современных установочных средствах. Особое внимание уделяется повышению осведомленности пользователей о методах обмана, используемых разработчиками НПО.

**Ключевые слова.** Установочные средства, программное обеспечение (ПО), пользовательский опыт, согласие пользователя, безопасность, нежелательное ПО (НПО), установка программного обеспечения, параметры согласия, прозрачность.

В эпоху цифровизации и все увеличивающегося потока данных, эффективность и прозрачность установочных средств становятся ключевыми факторами, определяющими пользовательский опыт и доверие. Установочные средства – это не просто технические механизмы для загрузки программного обеспечения, но и важные инструменты для взаимодействия с пользователем, которые могут существенно повлиять на восприятие продукта и доверие к разработчику. Однако, рынок этих средств демонстрирует значительное разнообразие подходов, начиная от простых и интуитивно понятных интерфейсов, и заканчивая сложными и многоуровневыми системами, требующими высокой степени вовлеченности от пользователя.

Особое внимание в современной практике уделяется методам получения согласия на обработку данных пользователя, что стало особенно актуальным после введения таких нормативных актов, как Общий регламент по защите данных (GDPR). Средства согласия должны не только соответствовать юридическим требованиям, но и быть максимально удобными и понятными для пользователей. В то же время, значительная часть программных продуктов до сих пор использует так называемые "нежелательные галочки" – предварительно установленные параметры, которые ведут к загрузке дополнительного, часто нежелательного программного обеспечения. Эта практика не только ухудшает пользовательский опыт, но и подрывает доверие, что ставит под вопрос этические аспекты таких методов.

По данным исследования Malwarebytes за 2023, около 73% пользователей столкнулись с нежелательным ПО (НПО) [1]. Это означает, что из 10 пользователей 7 человек установили на свои устройства нежелательное программное обеспечение, которое может нанести вред их компьютерам или украсть личные данные. В основном, это происходит из-за невнимательности пользователей, которые не читают условия установки перед тем, как нажать "Далее". Разработчики НПО прибегают к различным сомнительным методам, чтобы навязать свои программы ничего не подозревающим пользователям. НПО часто прячется в мелких, незаметных галочках, которые легко пропустить при установке других программ. Разработчики могут по умолчанию ставить галочки напротив согласия на установку их программ, вынуждая пользователей соглашаться, не читая условия. Условия установки программного обеспечения могут быть написаны сложным, юридическим языком, вводя пользователей в заблуждение и делая их уязвимыми.

С самого начала эры компьютерных технологий процесс установки программного обеспечения (ПО) прошёл значительную трансформацию. Ранние методы установки ПО часто требовали от пользователей глубоких технических знаний и включали в себя ручное копирование файлов с дискет или CD-ROM. Эти методы были трудоёмкими и подвержены ошибкам из-за сложности процедур и ограничений раннего программного и аппаратного обеспечения.

С развитием операционных систем и улучшением пользовательского интерфейса процесс установки стал более автоматизированным и дружелюбным к пользователю. Появление установочных мастеров (wizards) позволило автоматизировать процесс, предлагая пользователю простую последовательность шагов с выбором компонентов, места установки и других параметров. Это значительно упростило процедуру установки и сделало её более доступной для неспециалистов.

Первые методы установки ПО часто не учитывали безопасность, что становилось проблемой с увеличением числа вредоносного ПО и кибератак. Например, ранние установщики могли не проверять подлинность источника, что открывало возможности для атак типа "man-in-the-middle". В ответ на эти вызовы разработчики начали внедрять функции проверки целостности и подписывания кода, что позволило убедиться в надёжности и безопасности устанавливаемого ПО.

С течением времени установочные средства также адаптировались к изменениям в законодательстве о защите данных и приватности пользователей. Введение таких стандартов, как GDPR в Европейском Союзе, потребовало изменений в установочных средствах, включая более ясные

требования к согласию пользователя и улучшенное уведомление о том, какие данные собираются и как они будут использоваться.

Современные подходы к сбору согласий пользователя на обработку его данных значительно различаются в зависимости от целей, удобства пользователя и юридических требований. Рассмотрим основные методы:

Активное согласие (Opt-in): Этот метод требует, чтобы пользователь активно выразил своё согласие на обработку данных, например, поставив галочку в соответствующем поле. Это считается золотым стандартом в области защиты персональных данных, поскольку гарантирует, что согласие было дано осознанно.

Пассивное согласие (Opt-out): В этом случае согласие считается полученным, если пользователь не предпринял активных действий для его отказа. Например, предустановленные галочки, которые пользователь должен снять для отказа от определённых услуг или обработки данных. Этот метод часто критикуется, так как он может не отражать истинное желание пользователя.

Неявное согласие: Иногда согласие предполагается на основании действий пользователя, например, продолжение использования веб-сайта. Такой подход становится всё менее приемлемым в свете современных требований к ясности и однозначности согласий.

Использование предустановленных галочек (pre-selected checkboxes) в установщиках программного обеспечения является распространённой практикой среди разработчиков ПО. Этот метод часто применяется для продвижения дополнительных компонентов, таких как тулбары для браузеров, дополнительные приложения и сервисы, которые могут быть не совсем необходимы пользователю. Основная причина использования таких галочек — экономическая выгода. Разработчики и компании получают доход от сторонних поставщиков за каждую установку дополнительного ПО. Это создаёт стимул включать их в установочные пакеты, часто без явного информирования пользователя о последствиях такой установки.

Экономическая выгода от предустановленных галочек в установщиках ПО может привести к использованию так называемых "dark patterns" или "тёмных паттернов" в дизайне пользовательского интерфейса. "Предварительный выбор" является одним из таких тёмных паттернов, где по умолчанию выбраны опции, которые не обязательно являются наилучшим выбором для пользователя. Часто такие галочки предлагают установить дополнительные приложения или изменить настройки браузера, что может привести к неожиданным изменениям в системе или даже к угрозам безопасности [2].

Разработчики ПО часто прибегают к различным методам, чтобы склонить пользователей к установке ненужных компонентов, дополнительных программ, тулбаров для браузеров, антивирусов и т.д. Рассмотрим различные типы установщиков, использующие методы обмана для скачивания нежелательного ПО.

1 Метод "Принять/Отклонить".

Это один из распространенных методов обмана, используемых в установщиках ПО. Данный метод продемонстрирован на рисунке 1.

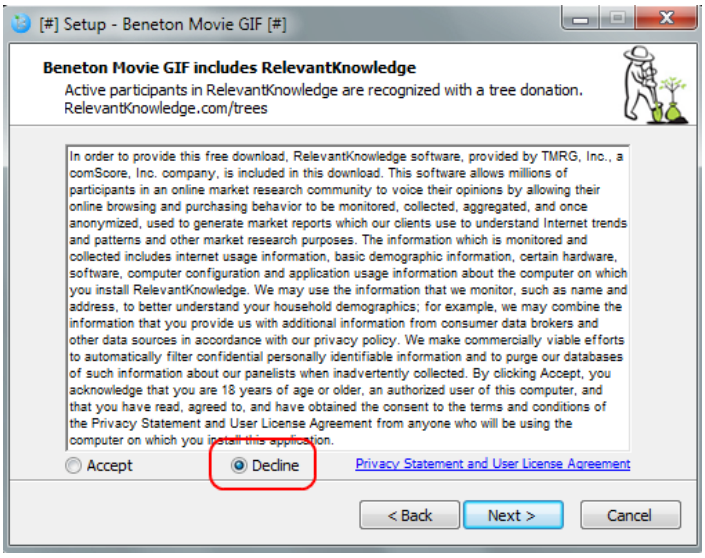


Рисунок 1 – Установщик с методом обмана "Принять/Отклонить"

Кнопка "Принять/Согласиться" обычно означает, что пользователь соглашается с установкой нежелательного ПО. Окно установщика в таком методе обычно имеет вводящий в заблуждение текст, который может выглядеть как лицензионное соглашение. Не все пользователи будут внимательно читать текст, особенно если он длинный и сложный.

2 Метод "Я согласен с...".

Данный метод использует подмену согласия. На рисунке 2 показан пример такого установщика.

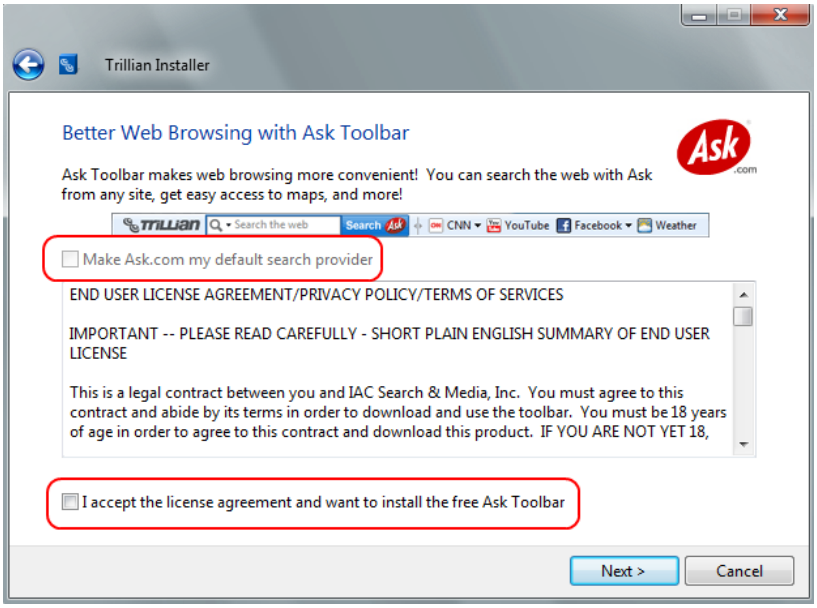


Рисунок 2 – Установщик с методом обмана "Я согласен с..."

Пользователь видит текст "Я согласен с лицензионным соглашением и хочу установить бесплатную панель Ask Toolbar". Однако, если пользователь не снимет флажок с "Установить Ask.com в качестве моего поискового провайдера по умолчанию", то Ask.com будет установлен как поисковая система по умолчанию для его браузера. Пользователя вводят в заблуждение, предоставив ему текст соглашения таким образом, чтобы он думал, что соглашается на установку только основного ПО.

3 Метод "Использование невнимательности пользователя".

На рисунке 3 показан установщик, предлагающий "Выборочную установку".

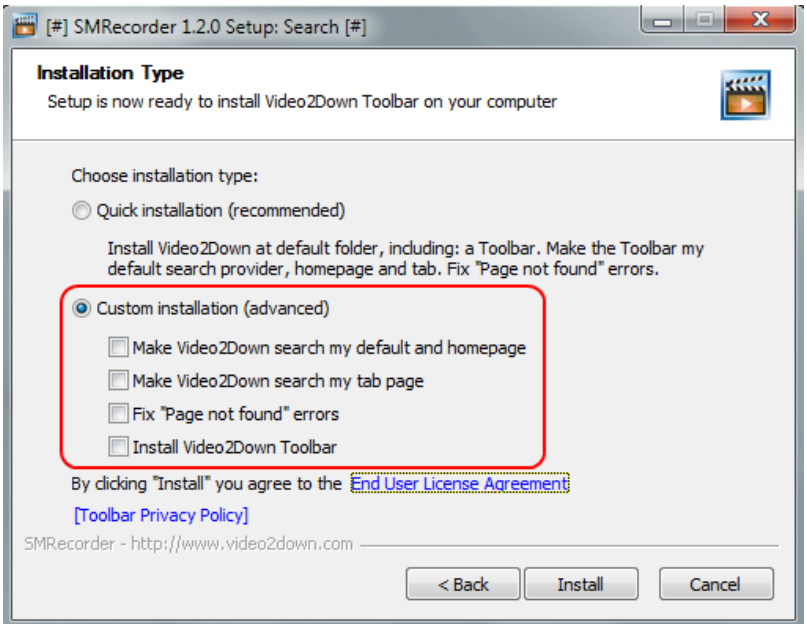


Рисунок 3 – Установщик с методом обмана "Использование невнимательности пользователя"

Еще один установщик с подменой согласия для распространения НПО. В этом методе разработчики ПО используют невнимательность пользователей, которые не снимают флажки с компонентов, которые им не нужны. В данном случае, если пользователь не снимет галочку с "Установить Video 2Down Toolbar", то этот нежелательный тулбар будет установлен на его компьютер.

4 Метод "Пост-установочный обман".

Этот установщик пытается поймать пользователей к установке ненужных компонентов уже после завершения установки основного ПО. Пример такого установщика изображен на рисунке 4.

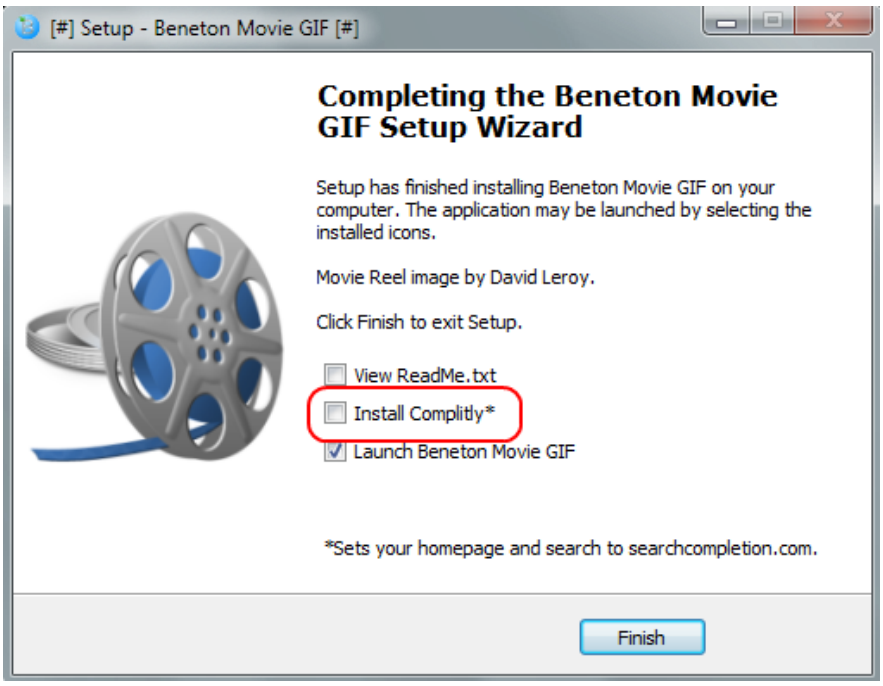


Рисунок 4 – Установщик с методом обмана "Пост-установочный обман"

Если пользователь не снимет флажок с "Установить Complitly", то этот компонент будет установлен на его компьютер. Галочки по умолчанию установлены напротив ненужных компонентов, и пользователь должен их самостоятельно снять, чтобы отказаться от установки.

5 Метод "Введение в заблуждение".

Даже при выборе "Выборочной установки" и снятии всех нежелательных галочек пользователь может установить ненужное ПО, если не будет внимателен. Это делается путем отвлекающего фактора, как на рисунке 5.

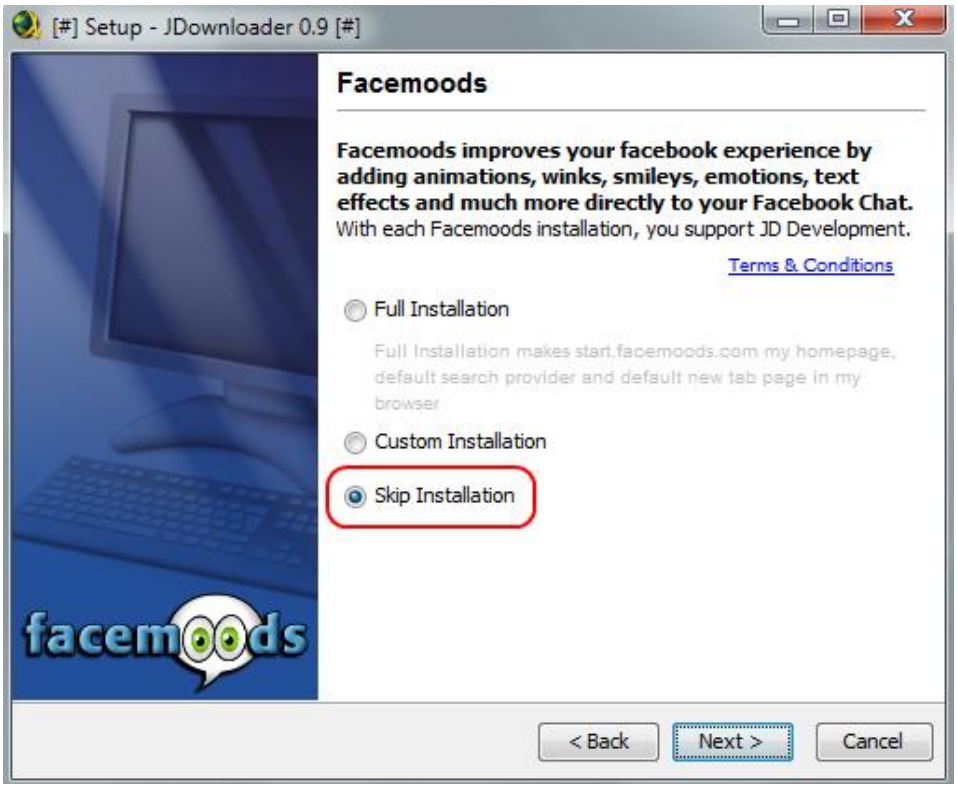


Рисунок 5 – Установщик с методом обмана "Введение в заблуждение"

Пользователи, полагая, что "Выборочная установка" дает им полный контроль над процессом, могут бегло выбрать ее, не обращая внимания на детали. В результате ненужные компоненты устанавливаются на устройство пользователя, зачастую без его осознанного согласия.

Для избежания непреднамеренной установки дополнительного ПО, существуют специальные программы, такие как Unchecky. Эта программа автоматически снимает предустановленные галочки во

время установки другого программного обеспечения, помогая таким образом предотвратить установку потенциально нежелательных программ или изменений в браузере.

Оценивая разнообразие установочных средств на рынке и доступных методов взаимодействия с параметрами согласий, можно сделать вывод, что установщики программного обеспечения значительно эволюционировали. Они предлагают различные уровни настройки и предварительно установленные параметры, которые могут как улучшать пользовательский опыт, так и вводить в заблуждение.

Несмотря на существование инструментов, таких как Unchecky, помогающих избежать непреднамеренной установки нежелательных программ, проблема обеспечения информированного согласия пользователя и прозрачности процесса установки остается актуальной.

Важным выводом является то, что на рынке недостаточно утилит, способных надежно защитить пользователей от ненужных установок. В связи с этим разработка усовершенствованных утилит для снятия галочек, подобных Unchecky, представляет собой актуальную задачу, требующую дальнейших исследований.

***Список использованных источников:***

*1. Исследование Malwarebytes за 2023 год [Электронный ресурс]. – Режим доступа: https://www.mrg-effitas.com/wp-content/uploads/2023/06/MRG_Effitas_360_Q1_2023_Final.pdf. – Дата доступа: 20.04.2024.*

*2. Deceptive Design. Types of Preselection [Электронный ресурс]. – Режим доступа: https://www.deceptive.design/types/preselection. – Дата доступа: 20.04.2024.*