**УДК 347.77**

# СТРАТЕГИЯ ЗАЩИТЫ ЦИФРОВОГО ПРОДУКТА НА ПРЕДПРИЯТИИ ОБЩЕСТВЕННОГО ПИТАНИЯ

**Попова Е.А.**
**Консультант – магистр Бойцова Ю.С.**
**Научный руководитель – к.т.н., доцент Орлова О.Ю.**
Университет ИТМО

*Аннотация:* в работе рассмотрены основные способы защиты цифрового продукта на предприятии общественного питания, такие как патент, авторское право, товарный знак, торговый секрет, соглашение о конфиденциальности, условия обслуживания. Выявлены самые популярные и реализуемые в России: составление и подписание договоров о неразглашении информации, разграничение уровней доступа для сотрудников, разработка специального ПО. Проанализированы источники угроз потери персональных данных IT-стартапа, такие как антропогенные и техногенные. Таким образом, благодаря исследованию освещена тема стратегий защиты продукта общественного питания, даны рекомендации для управления интеллектуальной собственностью на стыке современного общества и трендов.
*Ключевые слова:* патент, коммерческая тайна, ноу-хау, IT-стартап, товарный знак.

## Введение

Интеллектуальная собственность давно признана ключевым и практически неисчерпаемым ресурсом экономики. Но сегодня она становится еще и инструментом развития цифровых технологий, формирует самостоятельный, глобальный цифровой рынок. Россия за время пандемии сделала огромный шаг в развитии интеллектуальных систем и внедрении цифровизации на предприятия общественного питания. По мере развития и внедрения цифровых технологий в сфере фудтеха, встает немаловажный вопрос о защите интеллектуальной собственности, будь то мобильное приложение или технология роботизированного производства. Так же, интеллектуальная собственность часто является наиболее ценным активом IT-стартапа. Поэтому защита интеллектуальной собственности имеет большое значение для получения венчурного финансирования или предотвращения несправедливой конкуренции.

Цель данного исследования выбор оптимального и эффективного способа защиты информации в сфере фудтеха.

В соответствии с целью будут решены следующие задачи:
– рассмотрены основные источники угроз для фудтех - IT-стартапа;
– изучены основные способы защиты информации в условиях современной России;
– проведен анализ самых эффективных стратегий по защите цифровой информации.

## Результаты

Основной задачей применения защиты интеллектуальной собственности – это защита от угроз. Рассмотрим возможные угрозы в стартап-проектах:

1. Антропогенные источники угроз

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние. Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся: потенциальные преступники и хакеры, недобросовестные партнеры, представители надзорных организаций и аварийных служб,

представители силовых структур.

Внутренние субъекты представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся: основной персонал (пользователи, программисты, разработчики), представители службы защиты информации, вспомогательный персонал (уборщики, охрана), технический персонал (жизнеобеспечение, эксплуатация).

2. Техногенные источники угроз

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Технические средства, являющиеся источниками потенциальных угроз безопасности: некачественные технические средства обработки информации, некачественные программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии).

Самый значимый элемент стратегии защиты интеллектуальной собственности – оптимальный выбор средств защиты. Ниже представлены самые распространенные из них:

1. Патенты – дает его изобретателю право запрещать другим лицам производить, использовать или продавать запатентованный объект, описанный словами в формуле изобретения.

2. Авторские права распространяются на оригинальные авторские произведения. К ним, в том числе, относится и программное обеспечение (код). Авторское право дает владельцу исключительное право делать копии произведения и готовить производные. Кроме того, можно вынести владение авторскими правами (например, кодом) в отдельный вид деятельности, зарегистрировать для этого отдельную компанию в стране, которая привлекает обладателей квалифицированных активов (IP box) пониженными налоговыми ставками на прибыль за использование подобных прав. К таким странам относятся. например: Кипр (2.5%), Польша (5%), Венгрия (4.5%) и с 2020 года — Швейцария (но только по изобретениям, защищенным патентом)

3. Право на товарный знак или марку защищает символическое значение слова, имени, символа или устройства, которое владелец товарного знака использует для идентификации или отличия своих товаров от товаров конкурентов. Некоторые товарные знаки известны всему миру, как например: товарный знак Intel, BMW или Nike. Компания получает права на товарный знак, фактически используя его в торговле.

4. Торговые секреты или коммерческая тайна могут быть отличным активом для стартапов. Они экономически эффективны и действуют до тех пор, пока коммерческая тайна сохраняет свой конфиденциальный статус и получает ценность благодаря своей секретности. Коммерческие секреты могут варьироваться от компьютерных программ до списков клиентов и формулы для Coca-Cola

5. Соглашения о конфиденциальности. Целью подобного соглашения является предоставление держателю конфиденциальной информации (такой как продукт, услуга или бизнес-идея), чтобы он не мог поделиться ею с третьей стороной.

6. Условия обслуживания и Политика конфиденциальности. Если компания ведет свою деятельность в Интернете, важно иметь соглашение об условиях обслуживания, которое ограничивает действия пользователей на веб-сайте. Например, создание и использование групповых и общих учетных записей.

Самым актуальными на сегодняшний день в России способом защиты цифрового продукта являются соглашение о неразглашении конфиденциальной информации, внимательный подбор сотрудников, а также условия их работы, реже авторское право и патент.

**Заключение**

В работе проведено исследование основных способов защиты интеллектуальной собственности в сфере фудтеха. Важно не пренебрегать изученными выше способами. В 2022 году продолжается гонка предприятий общественного питания за увеличение прибыли и оптимизацию производства путем внедрения цифровых технологий. Успех ждет то предприятие, которое не только раньше всех внедрит новые технологии, приложения, но и сумеет качественно защитить свои разработки.