**StartUp – проекты цифровизации экономики и образовательной сферы**

**DIGITAL ECONOMY AND EDUCATION STARTUPS**

Соловьева М. А.

Санкт-Петербургский государственный экономический университет,

г. Санкт-Петербург, Россия

Исследованы ключевые аспекты развития стартапов в процессе цифровизации экономики, в том числе образовательной сферы. Отдельный акцент сделан на значимости стартапов в области защиты информации, как основы обеспечения стабильного развития цифровых сервисов. Выделены наиболее перспективные стартапы в области защиты от веб-фишинга и кардинга. Проанализирована структура атак на физические и юридические лица по объектам и методам атак.

Ключевые слова: стартап, информационные технологии, кибербезопасность, фишинг, цифровизация

The article examines the key aspects of the development of startups in the process of digitalization of the economy, including the educational sphere. Special attention is paid to the importance of startups in the field of information security as the basis for ensuring the stable development of digital services. The most promising startups in the field of protection from web-fishing and carding are highlighted. The structure of attacks on individuals and legal entities by objects and methods of attacks is analyzed.

Keywords: startup, information technologies, cybersecurity, fishing, digitalization

Одним из ключевых критериев конкурентоспособности экономики в современном мире является уровень её цифровизации. Цифровизация – процесс внедрения цифровых технологий для повышения уровня социальной и экономической сфер общественной жизни. Под этим термином подразумевается трансформация информации в цифровую форму, что делает данные более доступными для пользователей. Основными инструментами цифровизации являются BigData, машинное обучение, нейронные сети, ИИ и т. д. Необходимо отметить, что цифровизация – неотъемлемая часть цифровой экономики, так как она является инфраструктурой и инструментальной базой. Именно цифровые технологии создают вектор развития экономики и способствуют повышению уровня жизни общества. Большинство стран, занимающих лидирующие позиции в мире, уделяют большое внимание цифровизации экономики. По данным компании IMD, наибольший уровень цифровизации наблюдается у США, Сингапура и Швеции. Россия находится на 38 месте[[1]](#footnote-1).

Под цифровой экономикой в научной литературе подразумевают комплекс экономической деятельности, направленный на разработку и внедрение ИКТ в работе с данными. Цифровая экономика повышает конкурентоспособность, стимулирует инновации, что в целом обеспечивает высокую эффективность, производительность и качество товаров и услуг представляемых на потребительском рынке, а также реализует электронную торговлю, посредством Интернета. Цифровизация экономики создает эффективную систему сбора, обработки и хранения данных, обеспечивающих потребности граждан, организаций и государства.

Образно говоря, развитию цифровизации экономики способствуют уникальные идеи, посредством которых появляются новые технологии, обеспечивающие ее полноценное развитие. Под уникальной идеей имеется в виду проект, направленный на внедрение новых мыслей и извлечение прибыли путем привлечения денег инвесторов. Иначе говоря, Start-Up. Происхождения стартапа как бизнеса уходит в 70-е годы XX века.

Наиболее уязвимым элементом цифровизации экономики и, в частности, её образовательной сферы является обеспечение безопасности передачи данных. Упрощение обмена информацией с развитием цифровизации снижает уровень трансакционных издержек в экономике, но в то же время существенно увеличивает риски утечки информации. В связи с этим наибольшее внимание следует уделять стартапам в области кибербезопасности. По оценкам различных источников, рынок кибербезопасности составляет около $100 млрд, а по к 2024 году эта сумма может превысит $300 млрд.

На сегодняшний день существует множество стартапов в области кибербезопасности, но можно выделить самые перспективные, которые застрагивают все аспекты кибербезопасности, в том числе анализ угроз, loT, блокчейн, ИИ и машинное обучение.

За последнее десятилетие число и уровень сложности кибератак со стороны как прогосударственных хакерских групп, так и финансово мотивированных киберпреступников значительно возросли. С каждым годом схемы мошенничества совершенствуются, становятся более изощренными. Согласно отчету Positive Technologies за 2019 год «утечка персональных данных в результате кибератаки — по-прежнему одна из актуальных угроз». За прошлый год получение данных было целью 60% от всех атак на юридических лиц и 57% - на физических лиц. Персональные данные среди атак на данные были целью в 27% случаев при атаках на юридические лица и 12% - на физические лица.

Объектами атак являются не только компьютеры, серверы, сетевые оборудования, но и веб-ресурсы, люди, банкоматы и POS-терминалы, мобильные устройства, loT. Подавляющее большинство атак направлено именно на компьютеры, серверы и сетевое оборудование: 71% от всех атак на юридические лица. Скорее всего это связано с утечкой учетных данных через фишинговые сайты, где сотрудники компании, не подозревая ничего, переходили по ссылкам полученных писем злоумышленников, тем самым предоставляли им возможность реализации задуманных махинаций.

Что касается частных (физических) лиц, то не сильно велика разница между атаками, совершенными на компьютеры (32%), мобильные устройства (26%) и веб-ресурсы (31%). В целом, хотелось бы отметить, что в 2019 году, согласно отчету Positive Technologies, 19% от всех совершенных атак были направлены против частных лиц, то есть практически каждое пятое преступление[[2]](#footnote-2).

Самой частой категорией, подвергающейся кибератаке, являются государственные учреждения – 18%, а также компании из сферы науки и образования – 18%. Также можно отметить, что промышленные компании тоже достаточно в большом количестве подвергаются интернет-мошенничеству – 5%. Наиболее редкие категории жертв составляют блокчейн-проекты, телекоммуникационные компании, сферы услуг, транспорт, торговля и т.д.

Также существуют различные методы атак: использование вредоносного ПО, подбор учетных данных, социальная инженерия, хакинг, эксплуатация веб-уязвимости.

Использование вредносоного программного обеспечения пользуется самым популярным (занимает три четверти) методом кибератак по отношению к юридическим лицам, они составляют 66%. Социальная инженерия находится на втором месте атаки на юридических лиц– 51%, а по отношению к частным лицам – на первом – 63%.

Веб-фишинг - один из самых старых и простых видов мошенничества, который часто используют разные злоумышленники. Постепенно он заменяет собой сложные атаки с использованием дорогостоящих троянов или инструментов для взлома. Одна из причин популярности фишинга — простота реализации, однако он тоже эволюционирует. В большинстве случаев фишинг заключается в организации массовых рассылок электронных писем якобы от имени существующих крупных компаний, банков.

Антифишинговые стартапы являются одними из самых востребованных, для инвестиций. IRONSCALES – стартап, работающий для разработки борьбы с фишингом. Он представляет собой комплексную платформу, разработанную для быстрого обнаружения фишинговых электронных писем, которая автоматически реагирует на них и блокирует за считанные секунды. Так, разработанная ими программа помогла Dalton State University решить проблемы с угрозами безопасности электронной почты, тем самым сохранив $1,3 млн на найм 20 новых сотрудников.

Другой стартап Vade Secure, основанный в 2009 году в Бостоне, Массачусетс. Сейчас это мировой лидер: защищает 600 млн почтовых ящиков в 76 странах. Их цель – разработка технологий, выявляющих и блокирующих вредоносные ссылок и программ. Также защитить пользователей электронной почты от современных угроз. 10 млрд писем анализируется в день, 800 млн фишингов было обнаружено и 200 млн вредоносных программ в 2018 году.

Отдельно стоит выделить развитие стартапов в области защиты от кардинга – кражи данных банковских карт физических и юридических лиц. Отдельно отмечается значимость стартапа Marqeta, который смог привлечь финансирование в размере $116 млн. Компания предоставляет решение по выпуску и контролю за работой банковских карт.

На фоне быстрого развития информационных технологий необходима активная поддержка появляющихся стартапов в области защиты данных. В связи с этим, огромное значение имеет создание условий для развития появляющихся и существующих проектов, направленных на разработку новых методов, программ защиты. Например, центр «Сколково» является хорошей платформой, которая выделяет значительные суммы на развитие самых перспективных стартапов в области IT, что благоприятно влияет на условия для развития рынка IT в целом.

Подведя итоги, мы пришли к выводу, что одной из наиболее важных сфер развития стартапов в условиях цифровизации экономики и образовательной сферы является кибербезопасность. Учитывая масштабы атак на критически важную для развития цифровых сервисов инфраструктуру, в т.ч. государственную (четверть от всех атак), развитие стартапов в этой области – необходимое условие дальнейшего стабильного развития экономики и образовательной сферы страны.

**Список литературы:**

1. Официальный сайт компании IRONSCALES <https://ironscales.com/>

2. Официальный сайт компании Marqeta <https://www.marqeta.com/>

3. Официальный сайт компании Vade Secure <https://www.vadesecure.com/en/>

4. Group IB – HI-TECH CRIME TRENDS 2019/2020 – C.8-13

5. IMD World Digital Competitiveness Ranking. – С. 15-19.

6. Positive Technologies Актуальные киберугрозы 2019

7. Халин В. Г., Чернова Г. В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски //Управленческое консультирование. – 2018. – №. 10 (118).

8. Шеремет И. А. Цифровая экономика и кибербезопасность ее финансового сегмента //Научные труды Вольного экономического общества России. – 2018. – Т. 210. – №. 2. – С. 23-34.

1. IMD World Digital Competitiveness Ranking 2019, С.26-27 [↑](#footnote-ref-1)
2. Positive Technologies Актуальные киберугрозы 2019. С. 5-11 [↑](#footnote-ref-2)