# ПРОБЛЕМЫ СОВРЕМЕННОЙ КИБЕРБЕЗОПАСНОСТИ

***Задорожнюк Н. А., к. э. н., доцент,***
***Зубков В. А., студент***
***Одесский национальный политехнический университет***

Чтобы экономика региона, страны и мирового сообщества в целом могла получать коммерческую выгоду от технологических инноваций в полной мере, необходимо обеспечить надежный и скоординированный подход к кибербезопасности.

В отчете Всемирного экономического форума за 2018 год [1] отмечено, что кибератаки стали более опасными и распространёнными (занимают третью позицию в рейтинге самых вероятных угроз для национальной и глобальной экономики) и сравнимы с мошенничеством в технологическом аспекте.

Специалисты связывают кибератаки с такими возможными инцидентами:

- перебои и даже вывод из строя критической информационной инфраструктуры;
- ошибки и сбои финансовых механизмов или институтов;
- террористические атаки;
- различные виды мошенничества, кража и неправомерное использование данных физических и/или юридических лиц, документы коммерческой или государственной важности.

Решением проблем, связанных с кибератаками, занимается кибербезопасность – сравнительно новое направление, которое продолжает формироваться, в связи с чем наблюдается нехватка соответствующих специалистов.

Современные реалии ИТ-сферы и сферы национальной безопасности, учитывая частые кибератаки в мире, характеризуются постоянной (даже ежедневной) разработкой новых программ, модификацией старых программных продуктов,

изменениями в кодах и прочими действиями ведущих специалистов. Однако, все равно возникают ошибки (что обусловлено человеческим фактором главным образом), из-за которых продолжают осуществляться кибератаки и различные киберпреступления.

За последние пять лет количество кибератак, направленных на расшатывание бизнеса удвоилось, и инциденты, которые ранее считались необычными сейчас становятся «обыденными». При этом расширяются негативные последствия от взломов систем. Например, в 2017 году 64 % всех вредоносных электронных почтовых ящиков перенесли в себе различные вирусы-вымогатели, такие, как WannaCry (от него пострадали более чем 300 тыс. компаний в 150 странах) и NotPetya, (стал причиной значительных финансовых потерь, более чем 300 млн. долларов для некоторых пострадавших компаний) [1].

Другое направление, которое широко распространено сегодня в мире – это использование кибератак против критической инфраструктуры и стратегических индустриальных секторов. В самом худшем сценарии последствиями таких кибератак будет крах национальных экономических систем и серьезные нарушения в мировом сообществе.

Анализ статистических данных [1] свидетельствует об увеличении количества кибератак с 68 на каждую фирму в 2012 году до 130 в 2017 году. Также с каждым годом увеличивается количество вредоносных программ, которые продаются через Интернет. Соответственно возрастают размеры финансовых потерь от кибератак: компании теряют в среднем 14,75 млн. долларов в год. При этом прогнозируется, что в течении последующих пяти лет кибератаки принесут до 8 трлн. долларов.

Также следует отметить, что повышенная степень риска характерна для среднего и малого бизнеса, поскольку корпорации вливают огромную часть капитала в безопасность, что делает проникновение в такую систему становится затруднительным. В

соответствии с отчетом WEF [1] затраты на обеспечение кибербезопасности становятся обязательными для выживания среднего и крупного бизнеса.

Согласно Закону «Об основных принципах обеспечения кибербезопасности Украины» внедрения организационно-технической модели киберзащиты, как составляющей национальной системы кибербезопасности, осуществляется Государственным центром киберзащиты и противодействия киберугрозами. Ядром этой модели является Центр реагирования на киберугрозы Госспецсвязи. Важно отметить, что технологическая и аналитическая системы Центра созданы на базе новейших достижений ведущих ИТ-компаний мира, разработанные на уровне лучших мировых аналогов и являются одними из самых мощных систем в Европе [2].

Исследование проблемы кибербезопасности Украины позволяет сделать выводы о том, что для ее обеспечения необходимо разработать целый комплекс мероприятий, инфраструктур, технических средств, соответствующего программного обеспечения и организационно-юридических процедур, направленных на выявление, нейтрализацию и предотвращения киберпреступлений.

Таким образом, кибербезопасность это дорогостоящая, но очень важная графа расходов не только для населения и предпринимательского сектора, но и для государств. Не развивая данную отрасль, бизнес и государство в целом будут и дальше нести значительные финансовые потери от кибератак.

## Список использованных источников

1. Всемирный экономический форум [Электронный ресурс]. – Режим доступа: https://www.weforum.org/

2. Юскович-Жуковська В.І. Принципи захищеності кіберпростору України / В.І. Юскович-Жуковська // Матеріали Всеукр. наук.-практ. конф.

«Безпека соціально-економічних процесів в кіберпросторі», 27 березня 2019. – Київ : Київ. нац. торг.-екон. ун-т. – С. 77-78.

3. Парадигма інноваційного розвитку в умовах ринкової трансформації : монографія / Е. М. Забарна, О. М. Козакова, В. А. Чередниченко [та ін.] ; за заг. ред. Е. М. Забарної ; Одес. нац. політехн. ун-т. – Херсон : Олді-плюс, 2019. – 92 с. http://dspace.opu.ua/jspui/handle/123456789/8458

# ІНВЕСТИЦІЙНИЙ КЛІМАТ ЯК ФАКТОР РОЗВИТКУ СПІЛЬНИХ ПІДПРИЄМСТВ В УКРАЇНІ

***Корінний С. О., к. е. н., доцент,***
***Клінтухов О. О., студент,***
***Запорізький національний університет***

В сучасних умовах модернізації економіки України виникає необхідність розвитку спільного підприємництва з залученням іноземного капіталу. Організація та розвиток діяльності підприємств з іноземними інвестиціями є способом виходу держави з самоізоляції, засобом інтеграції її до світових систем господарювання і міжнародного розподілу праці. Підприємства за участю іноземного капіталу виступають найбільш прогресивною, конкурентоспроможною формою господарювання, інструментом формування ринкових відносин в економіці України.

Інтеграція України до світової системи господарювання є важливою умовою виходу на нові ринки збуту та зміцнення конкурентних переваг вітчизняних підприємств. Цей процес передбачає широке залучення і використання іноземного капіталу, що зумовлено недостатнім обсягом внутрішніх ресурсів, особливо у сферу, що визначається незадовільною конкурентоспроможністю на зарубіжних ринках. Перспективи успішної роботи багатьох вітчизняних підприємств та ефективність національної економіки загалом значною мірою