***Джерела та література***

1. Вядрова І. М. Система фінансового забезпечення інноваційного-інвестиційного розвитку в Україні та можливості її активізації в сучасних економічних умовах / І. М. Вядрова, С. М. Пашова // Вісник Університету банківської справи НБУ. – 2011. – № 1 (10). – С. 121–126.
2. Дегтярьова І. Б. Врахування екстернальних ефектів при розрахунку синергетичних результатів в еколого-економічних системах / І. Б. Дегтярьова // Механізм регулювання економіки. – 2009. – № 1 – С. 52–61.
3. Офіційний сайт підприємства ПАТ «РІВНЕАЗОТ» [Електроний ресурс]. – Режим доступу : http://www.azot.rv.ua/
4. Прокопенко О. В. Соціально-економічна мотивація екологізації інноваційної діяльності : монографія / О. В. Прокопенко. – Суми : Вид-во СумДУ, 2010. – 395 с.
5. Рюмина Е. В. Анализ эколого-экономических взаимодействий : [монография] / Е. В. Рюмина. – М. : Наука, 2000. – 158 с.

**Липич Любовь, Глубицкая Татьяна. Оценка эффективности вложения инвестиций в экологические проекты по синергетическим эффектам.** В статье выделены виды инвестиций в экологические проекты; проведен анализ методик оценки целесообразности вложения инвестиций. Определены дополнительные эффекты от капиталовложений в экологические проекты по сферам деятельности предприятия. Осуществлена оценка целесообразности усовершенствований системы водоподготовки питьевой воды по синергетическим эффектам.

**Ключевые слова:** экоинвестиции, синергетический эффект, эффективность.

**Lipych Lubov, Glubitska Tetiana. Evaluating the Effectiveness of Investment in Environmental Projects for the Synergistic Effect.** The author singled types of investments in environmental projects; analysis methodologies to assess feasibility of investment. Determined additional effects on investment in environmental projects in areas of the company. It assesses the feasibility of water system improvements drinking water synergistic effect.

**Key words:** environmental investment, effect of synergies, efficiency.

УДК 658(075.8)

**Владимир Гранатуров** – доктор экономических наук, профессор Одесской национальной академии связи имени А. С. Попова;
**Владимир Трапезников** – доктор юридических наук, доцент Одесского национального политехнического университета

# Киберпреступность как один из источников возникновения предпринимательских рисков

Выполнен анализ состава правонарушений, связанных с умышленным использованием в преступных целях компьютера, мобильных средств и способов связи, их программного обеспечения, подключенных к глобальной сети Интернет, сотовым операторам связи, объединяемых понятием «киберпреступления». Осуществлено деление этих преступлений на группы по содержанию, характеру и степени влияния на результаты предпринимательской деятельности. Показано, что по характеру влияния эти преступления прямо или косвенно (опосредовано) угрожают предпринимательской деятельности. Приведено обоснование состава рисков предпринимательской деятельности, источником возникновения которых являются киберпреступления, формирование их определений и места в системе классификации предпринимательских рисков.

**Ключевые слова:** предпринимательские риски, киберпреступность, компьютерные риски, определение терминов, классификация.

**Постановка проблемы и ее значение**. Как показывает опыт развития общественного производства, риск является характерным феноменом рыночной экономики и принадлежит к фундаментальным понятиям экономической теории. Поэтому изучению риска, построению и совершенствованию адекватного инструментария его анализа, моделированию, прогнозированию, а также учету при принятии управленческих решений посвящено значительное количество научных и методических работ.

Следует отметить, что разворачивающиеся процессы глобализации при наличии их бесспорных преимуществ порождают ряд болезненных проблем и вызовов. Сегодня предпринимательская

деятельность осуществляется в условиях усложнения причинно-следственных и функциональных связей между элементами современного рыночного механизма, возникающих под влиянием мощных социально-экономических, политических, организационно-технических и других факторов. Это усиливает неопределенность, конфликтность, многокритериальность условий функционирования предприятий, порождает новые риски, которым они могут подвергаться, требует постоянных глубоких и всесторонних исследований в этой сфере.

Одним из весомых факторов, оказывающих влияние на процесс воспроизводства неопределенности и риска предпринимательской деятельности, является киберпреступность. Распространение по всему миру ИКТ, предоставив человечеству принципиально новые решения и беспрецедентные возможности во всех сферах его жизнедеятельности, одновременно породило множество проблем, связанных с умышленным использованием в преступных целях компьютера, мобильных средств и способов связи, их программного обеспечения, подключенных к глобальной сети Интернет, сотовым операторам связи. Реальные и значительные риски, обусловленные несоответствием кибербезопасности и быстрым распространением киберпреступности, были признаны Всемирной встречей на высшем уровне по вопросам информационного общества, состоявшейся в два этапа (Женева, 2003; Тунис, 2005). Эта тенденция признана также Парламентской Ассамблеи ОБСЕ (Белград, 2011). В ее резолюции «Общий подход ОБСЕ к укреплению кибербезопасности», отмечалось, что угрозы, исходящие от киберпреступности постоянно эволюционируют и возрастают быстрым темпами. Несмотря на постоянное развитие средств защиты, количество киберпреступлений пока не снижается. Как отмечается в [1], за 2013 г. киберпреступники нанесли ущерб мировой экономике в размере $27 млрд против $18 млрд годом ранее (прирост на 50 %). В 2011 г. киберпреступникам удалось похитить у бизнеса и иных организаций примерно $12,5 млрд. Существует мнение, что киберпреступность приобрела характер глобальной индустрии, доходы которые по некоторым оценкам даже превышают $1 трлн и постоянно возрастают [2]. Как отмечается во Всемирном обзоре экономических преступлений за 2011 г., подготовленном компанией PricewaterhouseCoopers (PwC), киберпреступность стала одним из пяти самых распространенных экономических преступлений в Украине [3]. О темпах роста киберпреступности в Украине говорит тот факт, что в предыдущем обзоре (за 2009 г.) результаты в данной области не были выделены, ввиду незначительного количества зафиксированных случаев киберпреступности. Сказанное свидетельствует о том, что киберпреступность оказывает существенное влияние на конечные результаты предпринимательской деятельности и является одним из весомых источников риска этой деятельности. Это обстоятельство определяет актуальность исследования, посвященного анализу предпринимательских рисков, источником возникновения которых являются киберпреступления.

**Анализ исследований по этой проблеме.** Логично предположить, что, поскольку источником возникновения таких рисков являются киберпреступления, их следует отнести к криминально-правовым рискам. Как отмечалось нами в [4], в большинстве литературных источников по проблеме предпринимательских рисков криминально-правовые риски даже не упоминаются. Впервые описание этих рисков их определение и место в системе классификации предпринимательских рисков приведено в [5]. В представленной классификации эти риски рассмотрены как простые, такие, что вследствие принятых при классификации исходных предпосылок и допущений не подлежат дальнейшему делению. Результаты последующих исследований [4] позволили нам усовершенствовать эту систему классификации за счет включения в нее ряда рисков, входящих в состав криминально-правовых рисков. К сожалению, в составе этих рисков отсутствуют риски, источником которых непосредственно являются киберпреступления. Следует отметить также, что в современной научной литературе по проблеме рисков, в лучшем случае, встречается только упоминание таких рисков, их состав и анализ практически отсутствует.

**Целью данного исследования** является углубление существующих наработок по вопросам состава понятия «предпринимательский риск» путем анализа рисков, источником которых являются киберпреступления, а также их места в системе классификации предпринимательских рисков.

**Изложение основного материала и обоснование полученных результатов исследования.** Для выявления и обоснования состава рисков предпринимательской деятельности, источником которых являются киберпреступления, важным является определение понятия «киберпреступление», а также состав правонарушений, которые объединяются этим понятием. К сожалению, официального,

закрепленного в международных документах определения киберпреступности, состава и характеристики преступлений пока не существует. В настоящее время в литературе по киберпреступлениям и киберугрозам [6–9] нет согласованного мнения по этим вопросам. Вместе с тем, в большинстве случаев, различия касаются некоторых юридических тонкостей и деталей, которые, по нашему мнению, не оказывают существенного влияния на состав рисков, вызываемых этими преступлениями.

Нашему пониманию проблемы в наибольшей степени соответствует подход к определению этого понятия, изложенный в монографии Т. Л. Тропиной. Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [6]. При этом, как отмечает автор, в контексте данной работы использовано определение киберпространства, данное украинским ученым В. А. Голубевым. Киберпространство – это моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи [10].

Следует отметить, что термин «киберпреступность» в настоящее время часто употребляется наряду с термином «компьютерная преступность», причем нередко эти понятия используются как синонимы. Действительно, эти термины очень близки друг другу, но все-таки не синонимичны. Так, в рамках работы X конгресса ООН по предупреждению преступности и обращению с правонарушителями (Вена, 2000) специалистами ООН дано два определения киберпреступления – в широком и в узком смысле:

– киберпреступление в широком смысле (как преступление, связанное с компьютерами): любое противоправное деяние, совершенное посредством или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации посредством компьютерных систем или сетей;

– киберпреступление в узком смысле (компьютерное преступление): любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных [8].

Как видно из этих определений, термин «компьютерное преступление» относится только к преступлениям, совершаемым против компьютеров или компьютерных данных, в то время как киберпреступление в широком смысле охватывает как преступление против компьютеров и компьютерных данных, так и преступления, в которых компьютер является орудием или средством их совершения. В этом смысле компьютерное преступление следует рассматривать как разновидность киберпреступления.

В литературе по проблеме существует обширный перечень преступлений, которые авторы относят к киберпреступлениям или к их разновидности, компьютерным преступлениям, а также способы их классификации. Так, в Конвенции Совета Европы о киберпреступности [11] (с последующим дополнением) выделено следующие пять групп киберпреступлений:

– преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;

– преступления, связанные с использованием компьютерных средств;

– преступления, связанные с контентом (содержанием данных);

– преступления, связанные с нарушением авторского права и смежных прав;

– распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности.

В состав первой группы – преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем отнесены следующие виды преступлений:

– незаконный доступ – (ст. 2 Конвенции), противоправный умышленный доступ к компьютерной системе либо ее части;

– незаконный перехват – (ст. 3), противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах;

– вмешательство в данные – (ст. 4), противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных;

– вмешательство в систему – (ст. 5), противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных.

Как отмечает Т. Л. Тропина [6], именно эти четыре вида киберпреступлений «в чистом виде» являются компьютерными преступлениями. Остальные – это либо связанные с компьютером, либо совершаемые с помощью компьютера преступления. К ним относятся:

– преступления, в которых компьютер является орудием (электронные хищения, мошенничества, нарушение авторских прав и т. п.);

– деяния, при совершении которых компьютер является средством (например размещение на сайтах детской порнографии, клеветы, информации, разжигающей национальную, расовую, религиозную вражду и т. д.);

– деяния, направленные на безопасность общества и физическую безопасность, жизнь и здоровье человека (угроза физической расправы, кибертерроризм) и др.

Как видим, большинство из таких преступлений могут оказывать влияние на конечные результаты предпринимательской деятельности, внося в нее элементы неопределенности, т. е. являться источником риска. При этом возникает вопрос о составе рисков, источником которых являются киберпреступления, а также об их месте в системе классификации предпринимательских рисков.

Исходя из представленной нами в [4] классификации предпринимательских рисков, как отмечалось выше, логично предположить, что такие риски следует отнести к криминально-правовым рискам. По причинам возникновения криминально-правовых рисков, последствиями их наступления, а также возможными путями их предупреждения или снижения эти риски в системе классификации разделены на две группы – криминальные и административно-правовые риски.

К криминальным отнесены риски, которые являются следствием тяжких нарушений существующего законодательства и совершение которых, в соответствии с этим законодательством, предусматривает уголовную ответственность лиц, по вине которых возникли эти нарушения.

По характеру проявления криминальные риски поделены на:

– уголовные (грабеж, умышленное причинение вреда имуществу или здоровью предпринимателей, рэкет);

– коррупционные (рейдерство, взяточничество);

– мошеннические (внедрение различных схем присвоения чужих денег или имущества, частичного или полного уклонения от налогов и др.);

– преступной халатности (халатность должностных лиц, которая приводит к тяжким последствиям – гибель людей, экологическое загрязнение и т. п.).

К административно-правовым отнесены риски, которые являются следствием разных не тяжких умышленных или неумышленных нарушений субъектом хозяйствования существующего законодательства, за которые предусмотрена административная ответственность физических и юридических лиц, по вине которых возникли эти нарушения.

К таким нарушениям можно отнести:

– невыполнение персоналом требований пожарной безопасности, правил безопасности труда, санитарно-гигиенических норм и т. п.;

– различные неправомерные действия со стороны персонала и должностных лиц, которые не приводят к тяжелым последствиям;

– несвоевременная подача налоговой отчетности, арифметические и методические ошибки в налоговой отчетности, нарушение сроков оплаты налогов, сборов, обязательных платежей и т. п.

По характеру проявления и последствиям их возникновения административно-правовые риски могут быть поделены на риски умышленных и неумышленных нарушений законодательства.

Не трудно увидеть, что риски, источником которых являются киберпреступления, по характеру проявления и последствиями их возникновения относятся к криминальным рискам.

Для выводов относительно состава таких рисков, формирования их определений, а также их места в системе классификации необходимо сделать следующее замечание. По содержанию, характеру и степени влияния на результаты предпринимательской деятельности, по нашему мнению, можно выделить три группы киберпреступлений.

К первой группе следует отнести киберпреступления, которые по своей сути не являются новыми видами противоправных деяний, их составы, как правило, включены в национальное уголовное законодательство. Это традиционные преступления, совершенные с помощью компьютеров или в сети Интернет и которые не образуют новых составов преступлений (вымогательство, мошенничество, воровство и мн. др.). Риски, обусловленные этими преступлениями, подпадают под перечисленные выше подвиды криминальных рисков и, по нашему мнению, не требуют выделения их в отдельные подвиды.

Вторую и третью группу образуют киберпреступления, которые по своей сути являются новыми видами противоправных деяний и прямо или косвенно угрожают предпринимательской деятельности, а обусловленные ими риски не подпадают под перечисленные выше подвиды криминальных рисков.

Так, ко второй группе можно отнести компьютерные преступления. Широкое, можно даже сказать, абсолютно полное использование компьютеров в процессе осуществления предпринимательской деятельности приводит к тому, что группа преступлений, посягающих на конфиденциальность, целостность, доступность и безопасное функционирование компьютерных данных и систем – компьютерные преступления являются непосредственной угрозой результатам этой деятельности. Это дает нам основание считать целесообразным включение в состав криминально-правовых рисков новый подвид – компьютерный риск. Следует отметить, что с определенными оговорками и допущениями риски, обусловленные этими преступлениями, также можно было бы отнести к некоторым перечисленным выше подвидам криминальных рисков. Однако при выделении компьютерного риска в отдельную подгруппу нами также учитывались следующие обстоятельства. Эти преступления, как относительно новый достаточно специфический по своей природе вид преступной деятельности, требуют разработки и внесения в уголовное законодательство специальных норм, предусматривающих ответственность за посягательства на компьютеры, компьютерные сети и компьютерные данные. Для предупреждения или снижения отрицательных последствий наступления такого риска требуется применение специальных специфических мер и методов. Основанием выделения его в отдельную подгруппу также была необходимость обратить внимание руководителей предприятий на эту угрозу. Поскольку, как показали результаты Всемирного обзора состояния информационной безопасности в 2011 году, подготовленного PwC, как в Украине [3], так и во многих странах мира [12], руководители предприятий не уделяют должного внимания обеспечению кибербезопасности. По мнению авторов указанных обзоров, это может свидетельствовать лишь о том, что им неизвестно о рисках, которым киберпреступность подвергает их организации.

К третьей группе можно отнести киберпреступления, посягающие на общественную безопасность и общественную нравственность, а также разжигание национальной, расовой, религиозной вражды и т. п. Эти преступления косвенно (опосредовано) угрожают предпринимательской деятельности, а обусловленные ими риски не подпадают под перечисленные выше подвиды криминальных рисков. По своему характеру и направленности такие преступления, по нашему мнению, в большей степени подпадают под понятие странового риска, характеристика которого приведена в [5]. При этом отдельно выделять риски, обусловленные такими преступлениями, не следует. По нашему мнению, для их учета достаточно в методики оценки странового риска включить систему индикаторов, учитывающих характер и состояние таких преступлений.

Таким образом, выполненный анализ позволил дополнить криминально-правовые риски еще одним подвидом, таким как компьютерный риск. Не трудно увидеть, что включение этого подвида в состав системы классификации предпринимательских рисков не приведет к разрушению построенной ранее системы, а только лишь дополнит ее.

В рассматриваемой системе классификации предпринимательских рисков место компьютерного риска определяется из следующей цепочки родовой и видовой взаимосвязи рисков: предпринимательский риск – криминально-правовые риски – криминальные риски – компьютерный риск.

Для раскрытия понятия «компьютерный риск» нами использовано определение через род и видовое отличие, которое вытекает из такой последовательности:

– *предпринимательский риск* – это объективно-субъективная экономическая категория, характеризующая неопределенность конечного результата деятельности вследствие возможного влияния (действия) на него ряда объективных и/или субъективных факторов, которые не учитывались при его планировании;

– *криминально-правовые риски* – это составляющая предпринимательского риска, которая определяет возможность незапланированного изменения конечного результата деятельности вследствие проявления неправомерных действий (рэкет, умышленное причинение вреда, взяточничество, коррупция чиновников и др.);

– *Криминальные риски* – это составляющая криминально-правовых рисков, которая определяет возможность незапланированной смены конечного результата предпринимательской деятельности вследствие проявления тяжких нарушений существующего законодательства со стороны физических и юридических лиц;

– *компьютерный риск* – это составляющая криминальных рисков, которая определяет возможность незапланированной смены конечного результата деятельности вследствие проявления преступлений, посягающих на конфиденциальность, целостность, доступность и безопасное функционирование компьютерных данных и систем.

**Выводы и перспективы дальнейших исследований.** Выполненный анализ позволяет в определенной степени усовершенствовать существующую систему классификации предпринимательских рисков за счет включения в нее нового элемента. Введение в систему классификации компьютерного риска позволит в дальнейшем более плодотворно и эффективно использовать исследования, направленные на определение и обоснование перспективных направлений мониторинга и путей предупреждения или снижения этого риска.

По нашему мнению, дальнейшие исследования в этом направлении должны быть направлены на разработку системы индикаторов, учитывающих характер и состояние тех киберпреступлений, которые косвенно влияют на предпринимательскую деятельность, для использования их в методике оценки странового риска.

***Источники и литература***


1. Ференец В. Потери мировой экономики от киберпреступлений выросли в 1,5 раза в 2013 году / В. Ференц [Электронный ресурс]. – Режим доступа : http://www.cnews.ru/reviews/new/security2014/articles/poteri_mirovoj_ekonomiki_ot_kiberprestuplenij_vyrosli_v_15/
2. Kshatri N. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. – Heidelberg ; London : Springer, 2010. – 251 p.
3. Украина. Всемирный обзор экономических преступлений. Киберпреступления в центре внимания. – PwC, 2011. – 16 с.
4. Гранатуров В. М. Аналіз кримінально-правової складової підприємницьких ризиків / В. М. Гранатуров, В. І. Трапезніков // Вісник Чернівецького торговельно-економічного інституту. – Чернівці ; Луцьк : ЧТЕІ КНТЕУ, 2011. – Вип. ІІ (42). – Ч. 2. – Т.1 : Економічні науки. – С. 175–182.
5. Гранатуров В. М. Аналіз підприємницьких ризиків: Проблеми визначення, класифікації та кількісної оцінки : монографія / В. М. Гранатуров, І. В. Литовченко, С. К. Харічков ; за наук. ред. В. М. Гранатурова. – Одеса : Ін-т проблем ринку та економіко-екологічних досліджень НАН України, 2003. – 164 с.
6. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : монография / Т. Л. Тропина. – Владивосток : Изд-во Дальневост. ун-та, 2009. – 240 с.
7. Чекунов И. Г. Современные киберугрозы. Уголовно правовая и криминалистическая классификация и классификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2012. – № 1 [Электронный ресурс]. – Режим доступа : http://www.center-bereg.ru/o1102.html
8. Crimes related to computer networks. Background paper for the workshop on crimes related to the computer Network. A/CONF.187/10. – Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna, 10–17 April 2000.
9. Understanding cybercrime: Phenomena, challenges and legal response. – Geneva : ITU, Telecommunication Development Sector, 2012. – 356 p.
10. Голубев В.А. Кибертерроризм – миф или реальная опасность? [Электронный ресурс] / В. А. Голубев. – Центр исследования проблем компьютерной преступности. – Режим доступа : http://www.crime-research.org/library/terror3.htm
11. Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activity report. – Prepared by Committee of Experts on Crime in Cyber-Space (PC-CY) Submitted to European Committee on

Crime Problems (CDPC) at its 50 th plenary session (18 – 22 June 2001). – Secretariat memorandum prepared by the Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev 2. – Strasbourg, 20 June 2001.
12. Cybercrime: protecting against the growing threat. The Global Economic Crime Survey. – PwC, 2011. – 36 p.

**Гранатуров Володимир, Тропезников Володимир. Кіберзлочинність – одне із джерел виникнення підприємницьких ризиків.** Виконано групування кіберзлочинів, відповідно до їх впливу на появу ризиків підприємницької діяльності. Наведено обґрунтування складу ризиків, джерелом виникнення яких є кіберзлочини, формування їх визначень та місця в системі класифікації підприємницьких ризиків.
**Ключові слова:** підприємницькі ризики, кіберзлочинність, комп'ютерні ризики, визначення термінів, класифікація

**Granaturov Vladimir, Trapeznikov Vladimir. Cybercrime is one of the Sources of Entrepreneurial Risks.** The analysis of offences of willful criminal use of a computer, mobile communication means and methods of their software that are connected to the Internet, mobile communication operators that use the concept of «cybercrime». Distribution of these crimes carried in groups on the content, nature and degree of impact on business results. Shows that by the nature of the impact these crimes directly or indirectly (indirectly) threaten business. The substantiation of the composition of the entrepreneurial risks, which arise as a result of cybercrime. These definitions are formed and place in the system of classification of enterprise risks.
**Key words:** business risks, cybercrime, computer risks, definitions, classification.

УДК 65.012.

**Олена Стащук** – доцент кафедри фінансів і кредиту,
Східноєвропейський національний університет
імені Лесі Українки

# Теоретичні аспекти фінансової безпеки акціонерних товариств

У статті проведено огляд підходів науковців до розуміння поняття «фінансова безпека акціонерних товариств», запропоновано власний підхід до його розуміння Визначено характеристики фінансової безпеки акціонерних товариств, сформульовано основні її функції.
**Ключові слова:** акціонерні товариства, фінансова безпека, показники-індикатори фінансової безпеки, характеристики фінансової безпеки, функції фінансової безпеки.

**Постановка наукової проблеми та її значення.** У сучасних умовах функціонування економіки ефективне господарювання підприємницьких структур значною мірою залежить від їх здатності протистояти численним ризикам, що притаманні фінансовій діяльності підприємств. Негативні зміни стану економіки в цілому не забезпечують підприємствам стійкого економічного зростання та їх розширеного відтворення. Наявність у підприємства резервів, що дають змогу знівелювати негативний вплив факторів на результативність діяльності підприємств, відображається у формуванні системи їхньої фінансової безпеки.

Одна з важливих умов забезпечення зростання суб'єкта господарювання та формування позитивних результатів його фінансової діяльності – наявність ефективної системи фінансової безпеки, яка дасть змогу захистити підприємство від внутрішніх і зовнішніх загроз. Діяльність господарюючих суб'єктів економіки, незалежно від форми власності, пов'язана з наявністю ризику й формуються під впливом зовнішнього та внутрішнього середовищ їх функціонування. Підвищення рівня ризиків підприємницької діяльності вимагає від підприємств організації системи забезпечення їхньої фінансової безпеки, а також визначення основних факторів її формування.

Стан фінансової безпеки на підприємстві, на наше переконання, повинен формуватися залежно від типу, масштабу діяльності підприємства й з урахуванням особливостей існуючого на підприємстві організаційно-правового статусу діяльності суб'єкта господарювання. Найбільш поширена організаційно-правова форма ведення бізнесу в Україні – акціонерні товариства. Корпоративний сектор економіки забезпечує виробництво близько 70 % валового внутрішнього продукту України, що свідчить про його вагомий внесок у забезпечення економічного зростання країни. Актуальним питанням