5. Матишевський П.С. Кримінальне право України. Загальна частина / П.С. Матишевський. – К. : Юрінком Інтер, 2000. – 271 с.

6. Про прокуратуру. Закон України від 14 листопада 2014 року, № 1697 – 18 // Відомості Верховної Ради України (ВВР). – Ст. 99.

7. Бандурка О.М. Прокуратура: мысли о её реорганизации / О.М. бандурка // Право Украини. – 1999. – № 9. – С. 36–42.

8. Сухонос В.В. Организационно-правовые проблемы кадрового обеспечения органов прокуратуры / В.В. Сухонос, М.Е. Марочкин, В.В. Богуцкий. – Сумы : Слобожанщина. – 2000. – 220 с.

9. Сірий М. Про місце прокуратури в системі розподілу влади та джерела її функцій / М. Сірий // Реформування органів прокуратури України: проблеми і перспективи : Матеріали Міжнародної науково – практичної конференції (2–3 жовтня 2006 року). – К. : Академія прокуратури України, 2006.

10. Кодекс професійної етики та поведінки працівників прокуратури, схвалено Всеукраїнською конференцією працівників прокуратури від 28 листопада 2012 р., затверджено Наказом Генерального прокурора України від 28 листопада 2012 р. № 123 [Електронний ресурс]. – Режим доступу : http://www.gp.gov.ua/ua/kodet.html?_m=publications&_t=rec&id=113992.

11. Лакизюк В. Гласність в системі принципів організації та діяльності прокуратури України / В. Лакизюк, О. Михайленко, В. Малюга // Вісник прокуратури. – 2001. – № 4. – С. 11–21.

12. Резолюція 1755 (2010) Парламентської Асамблеї Ради Європи «Функціонування демократичних інституцій в Україні». Ухвалена у Страсбурзі (Французька Республіка) 4 жовтня 2010 року [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_a19.

13. Про внесення змін до Конституції України (щодо правосуддя). Закон України // Голос України. – № 118 (6372), середа, 29 червня 2016 року.

ПОРЯДОК ВНЕДРЕНИЯ ЗАЩИТЫ УЯЗВИМЫХ (БИОМЕТРИЧЕСКИХ) ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТАМИ ХОЗЯЙСТВОВАНИЯ НА ПРИМЕРЕ УКРАИНСКИХ ПРЕДПРИЯТИЙ

Юлия МЕДВЕДЕНКО,
аспирант кафедры правового регулирования экономики
ГВУЗ «Киевский национальный экономический университет
имени Вадима Гетьмана»,
юрист Юридической компании «Стратег»

Summary

The article analyses legal and regulatory framework of sensitive personal data protection on the example of the use of biometric personal data in the activity of Ukrainian businesses. The fundamental measures of ensuring the protection of sensitive personal data in the course of economic activity and administrating the work of an enterprise are defined on the example of specific business entities. In order to ensure reliable protection of sensitive personal data in combination with the process of optimization of everyday work of an enterprise the author presents her own algorithm of the method of implementation and usage of the technical processing of sensitive personal data in the work of business entities.

Key words: personal data, personal data protection, biometric personal data, economic entity.

Аннотация

В статье анализируется нормативно-правовое регулирование защиты уязвимых персональных данных на примере использования биометрических персональных данных в деятельности украинских коммерческих предприятий. Определяются основополагающие меры по обеспечению защиты уязвимых персональных данных в процессе осуществления хозяйственной деятельности и администрирования работы предприятий на примере конкретных субъектов хозяйствования. С целью обеспечения надежной защиты уязвимых персональных данных в сочетании с процессом оптимизации ежедневной работы предприятия автор предлагает собственный алгоритм методики внедрения и использования технической обработки уязвимых персональных данных в работе субъектов хозяйствования.

Ключевые слова: персональные данные, защита персональных данных, биометрические персональные данные, субъект хозяйствования.

Постановка проблемы. Сегодня процесс укрепления и повышения роли информационно-телекоммуникационных технологий нашел свое отображение во всех социальных, экономических и политических сферах деятельности. Стоит отметить, что вряд ли можно представить современную компанию, деятельность которой не включает процесс обработки информации о человеке: данные о сотрудниках, партнерах, клиентах, контрагентах. Очевидно, что какая-либо потеря, разглашение или несанкционированное изменение информации (включая базы персональных данных) может в последующем привести к невосполнимому ущербу, а иногда и к полной остановке деятельности компании. Не сложно представить себе размер убытков как финансовых, так и репутационных, например, для кредитно-финансовой или телекоммуникационной компании, которая потеряла хотя бы часть информации о своих клиентах. Достаточно вспомнить случай похищения 117 млн. паролей пользователей сервиса социальной сети LinkedIn, в результате чего были поставлены хакером на продажу пароли к доступу указанных аккаунтов (оценив примерно в 2,2 тыс. дол. США) [1], что послужило раскрытию персональных данных пользователей указанный социальной сети.

Актуальность темы исследования обусловлена недостаточной степенью изученности вопроса внедрения технической обработки и правового использования биометрических персональных данных в процессе работы украинских компаний. Актуальность темы также подтверждается в связи с растущей в Европе потребностью в повышении уровня безопасности относительно использования систем биометрической иденти-

фикации. В связи с тем, что украинский бизнес заинтересован в иностранных инвестициях, а также расширении границ бизнеса, включая европейские страны, возникает острая необходимость и важность разрешения вопроса создания эффективного механизма реализации гражданами своих прав и свобод в соотношении с качественным правовым регулированием деятельности компаний, которые используют персональные данные в своей работе.

Состояние исследования. Анализ проблемы защиты персональных данных в аспекте правового регулирования уязвимых персональных данных согласно украинскому законодательству исследует достаточно активно М.В. Ризак. Важно отметить, что несмотря на наличие достаточного количества научных исследований в области защиты персональных данных, конкретный правовой анализа состояния внедрения защиты биометрических персональных данных в рамках предприятия отечественными исследователями еще не проводился, что и обусловливает необходимость поиска и разработки практических рекомендаций для компаний, которые планируют использовать в своей деятельности базы биометрических персональных данных.

Целью и задачей статьи является анализ реального состояния защиты уязвимых персональных данных в процессе их использования в хозяйственной деятельности украинскими компаниями. Учитывая особое обострение проблемы безопасности международного оборота и обработки персональных данных, считаем необходимым исследовать состояние защиты уязвимых персональных данных украинскими субъектами хозяйствования, а также компаниями стран СНГ.

Изложение основного материала. Не вызывает никаких возражений тот факт, что неотъемлемой характеристикой современного общества является прогресс интеграции информационных технологий, а также интенсификация процессов в области информатизации. Эти факторы, как неотъемлемая часть процесса глобализации и построения информационного общества, одновременно порождают ряд проблем, связанных с необходимостью защиты личных прав и свобод человека, в частности в аспекте использования и обработки персональных данных [2]. В процессе поиска оптимальных механизмов обеспечения защиты конфиденциальной информации от несанкционированного доступа, а также эффективного контроля трудовой дисциплины предприятия начали внедрять инновационные технологии мониторинга на основе использования биометрических персональных данных. В докладе, представленном в августе 2015 года, аналитики Biometrics Research Group отметили рост спроса на биометрические приложения для управления труда, в том числе для решения задач оценки производительности труда и учета рабочего времени. Согласно докладу мировой рынок программного обеспечения для управления персоналом вырос с 10 млрд. дол. США в 2010 году до 18 млрд. дол. США к концу 2015 года. Рынок биометрических решений (как облачных, так и программно-аппаратных) достигнет 600 млн. дол. США в продажах к 2018 году [3].

Что касается правового регулирования данного вопроса, то стоит отметить, что украинское законодательство не запрещает использование указанной категории персональных данных, например, такие как биометрические данные сотрудников, партнеров, или контрагентов. В частности, работодатель имеет право вести систему учета рабочего времени работников, основанную на идентификации сканирования отпечатков пальцев, сканирования оболочек глаза, симметрии лица и т.д.

По состоянию на 2015 год, несмотря на тот факт, что Европа является вторым крупнейшим участником мирового рынка технологий биометрической идентификации по лицу, другие технологии, такие как распознавание отпечатков пальцев, рисунка вен на руке и радужной оболочки глаза, распространены шире. Внедрение систем facial recognition осуществлялось более низкими темпами, но аналитики ожидают, что в течение следующих четырех лет совокупные темпы годового роста этого рынка превысят 21% [4].

Важно отметить: невзирая на тот факт, что использование уязвимых персональных данных становится все более и более популярным в администрировании работы компании, но все также остается открытым вопрос соотношения эффективности использования таких данных и надлежащей защиты указанной категории данных. Сложность также заключается в том, что не все уполномоченные лица субъектов хозяйствования (которые отвечают за обработку персональных данных в рамках предприятия) могут четко разграничивать общие персональные данные субъекта и персональные данные, которые закон относит к уязвимым, вследствие чего они подлежать особенному порядку обработки и защиты.

Трудно не согласиться с мнением М.В. Ризака о том, что существенные проблемы в регулировании обращения уязвимых персональных данных обусловлены не только совокупностью данных, которые относятся к уязвимым согласно действующим нормам законодательства, но и разным подходом к регулированию обращения этих данных [5]. Так, исчерпывающий перечень биометрических данных человека в действующем законодательстве Украины, в частности Законе Украины «О защите персональных данных», отсутствует.

В соответствии с положениями статьи 6 Конвенции о защите лиц в связи с автоматизированной обработкой персональных данных от 28.01.1981 года к особой категории данных относятся персональные данные, свидетельствующие о расовой принадлежности, политических, религиозных или других убеждениях, а также данные, касающиеся здоровья или половой жизни. Они не могут подвергаться автоматизированной обработке, если внутреннее законодательство не обеспечивает соответствующих гарантий. Это правило также применяется к персональным данным, касающимся осуждения в уголовном порядке [6]. Стоит отметить, что Конвенция о защите лиц в связи с автоматизированной обработкой персональных данных 28.01.1981 года не относит к указанной категории персональных данных биометрические персональные данные человека. В свою очередь, положения части 1 статьи 7 Закона Украины «О защите персональных данных» запрещают обработку персональных данных о расовом или этническом происхождении, политических, религиозных или мировоззренческих убеждениях, членстве в политических партиях и профессиональных союзах, осуждениях к уголовному наказанию, а также данных, касающихся здоровья, половой жизни, биометрических или генетических данных [7]. Очевидно, что если Конвенция о защите лиц в связи с автоматизированной обработкой персональных данных от 28.01.1981 года не

включает биометрические персональные данные в категорию уязвимых, которые наделены особым статусом и подлежат особому режиму защиты, то законодательство Украины относит биометрические персональные данные к категории уязвимых, тем самым наделяя их повышенной степенью защиты.

Пункт 2 части 2 статьи 7 Закона Украины «О защите персональных данных» предусматривает, что запрет на обработку персональных данных не применяется, если обработка персональных данных необходима для осуществления прав и исполнения обязанностей владельца в сфере трудовых правоотношений в соответствии с законом и с обеспечением соответствующей защиты [7]. Для того, чтобы в соответствии с вышеуказанным пунктом Закона Украины «О защите персональных данных» субъект хозяйствования мог в своей хозяйственной деятельности или в процессе администрирования работы использовать базы уязвимых персональных данных, ему необходимо в пределах предприятия обеспечить надлежащий уровень защиты для использования такой категории персональных данных. Например, ООО «ГлаксоСмитКляйн Фармасьютикалс Украина» разработала для участников правила участия в Программе «Оранж кард», которая предусматривает собой сбор не только стандартных персональных данных клиента, но также и его биометрических данных. Это обусловлено, в первую очередь, тем, что программа сориентирована на пациентов, которые страдают от хронических заболеваний и нуждаются в препаратах ООО «ГлаксоСмитКляйн Фармасьютикалс Украина». Важно отметить, что указанные правила не имеют исчерпывающего перечня данных, которые компания может собирать и обрабатывать в дальнейшем, о пациенте, являющемся участником данной программы [8]. Согласно Политике ООО «Американ Экспресс Банк» в отношении обработки персональных данных установлено, что в компании подлежат обработке только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых в компании персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается. Важно отметить, что и в этом случае компания не указывает четкого перечня персональных данных, включая биометрические персональные данные, которые подлежат особому порядку защиты и обработки [9]. Аналогичную ситуацию можно отметить и в кодексе поведения при работе с персональными данными в АО «Киевстар». В указанном кодексе предусмотрено, что осуществление хозяйственной деятельности АО «Киевстар» предусматривает обработку персональных данных корпоративных абонентов компании, ее контрагентов и работников. Обработке подлежит информация, составляющая профиль потребления услуг, необходимая для осуществления трудовых отношений и хозяйственной деятельности в порядке, определенном законодательством [10].

Согласно официальной информации, размещенной на Интернет-ресурсе АО «БАЙЕР», к группе информации, которая в понимании компании относится к персональным данным, относится любая информация об определенном или определяемом физическом лице (субъекте персональных данных). Обработка биометрических персональных данных может осуществляться только после согласования с ответственным за организацию обработки персональных данных АО «БАЙЕР», юридическим отделом и менеджером по информационной безопасности компании и/или руководителем отдела Информационных Технологий. Данная обработка влечёт принятие специальных мер защиты согласно требованиям законодательства и корпоративной политики [11]. В свою очередь, АО «Арселор Миттал Темиртау» решило обеспечить более строгий порядок защиты персональных данных путем принятия Процедуры защиты данных, которая была официально утверждена Органом по защите данных ЕС. Настоящее Положение разработано в двух частях: Положение для субъектов данных (касающееся всех работников компании) и Положение для пользователей и работников компании, уполномоченных для работы с персональными данными. Согласно указанному Положению компания собирает и обрабатывает о каждом сотруднике объём персональных данных согласно перечню из 46 пунктов, два из которых включают информацию о биометрических персональных данных [12].

Пункт 1.2. Порядка уведомления Уполномоченного Верховной Рады Украины по правам человека об обработке персональных данных содержит информацию о том, что представляет особый риск для прав и свобод субъектов персональных данных, о структурном подразделении или ответственном лице, которое организует работу, связанную с защитой персональных данных при их обработке, а также об обнародовании указанной информации, утвержденном Приказом Уполномоченного Верховной Рады Украины по правам человека от 08.01.2014 года №1/02-14 (далее – Порядок от 08.01.2014 года №1/02-14) по отношению к кругу персональных данных, которые представляют особый риск для прав и свобод субъектов; определяется информация о персональных данных о биометрических данных и генетические данные лица [13].

Используя в деятельности предприятия базы данных, в которых используются биометрические персональные данные, необходимо обеспечить строгую систему контроля за обработкой такой информации. Заметим, что цепочка биометрической аутентификации может быть надежной только при условии, что процесс регистрации данных будет хорошо продуманным и организованным на локальном уровне.

Учитывая вышеизложенное, предлагаем авторский алгоритм методики внедрения технической обработки и использования биометрических персональных данных в работе субъектов хозяйствования.

Первым этапом должно стать внедрение средств технической обработки баз данных в рамках предприятия, что обязывает руководящий орган выдать акт в форме приказа по внедрению на предприятии технических считывающих устройств с использованием биометрических персональных данных «Об организации работ по обеспечению безопасности биометрических персональных данных, используемых на предприятии».

Для исполнения приказа должен быть назначен ответственный работник и/или сформирован соответствующий структурный отдел в пределах предприятия. На уполномоченного субъекта должна быть возложена обязанность по разработке правил обработки биометрических персональных данных, которые, в свою очередь, должны отвечать цели и правовому порядку обработки таких данных. Правила обработки биометрических персональных данных лиц должны включать в себя:

1. Четко определенный субъектный состав, который обеспечивает контроль за обработкой биометрических персональных данных на предприятии.

2. Сформированные методы контроля за порядком обработки персональных данных на предприятии, порядок фиксирования фактов нарушения обработки уязвимых персональных данных; определенный порядок и содержание мониторинга за соблюдением указанных Правил.

3. Закрепление функциональных обязанностей структурного подразделения, осуществляющего обработку уязвимых персональных данных, вовлеченных в процесс обработки.

4. Закрепление объёма ответственности за своевременность и правильность обработки персональных данных субъектов на предприятии, а также передачу данных для отражения в системе технического учета и идентификации личности должностным лицом структурного отдела, который осуществляет мониторинг и контроль за правовой обработкой биометрических персональных данных.

5. Порядок проведения внутренних проверок на предприятии. Проверки могут быть инициированы как руководящим органом предприятия, так и ответственным лицом и / или структурным подразделением. Указанные проверки могут быть разными по форме:

- внутренними. Предполагается установление соответствия обработки базы данных действующей нормативно-правовой базы, а также локальным актам;

- внешними (экспертная проверка). Привлечение независимых лиц для установления действительности обеспечения обработки биометрических персональных данных в рамках предприятия.

6. Определенные сроки выполнения разработки вышеуказанных Правил и порядок доведения его содержания к субъектам, персональные данные которых подлежат обработке.

7. Закрепленный порядок проведения технического обследования информационных систем накопления и считывания персональных данных в рамках предприятия. По результатам реализации процедуры в организации должно быть составлен Акт обследования информационных систем обработки персональных данных.

8. Установленный порядок получения разрешения на обработку биометрических персональных данных для обработки в компьютерных сетях и других технических устройствах, позволяющих обрабатывать и идентифицировать носителя данных. Должна быть определена форма и содержание согласия на обработку уязвимых персональных данных, а также алгоритм отзыва предоставленного согласия.

9. Утвержденный порядок внедрения системы защиты персональных данных. С точки зрения организационных мероприятий этот шаг должен включать в себя:

а) составление и утверждение перечня лиц, допущенных к обработке уязвимых персональных данных (в частности, работников службы безопасности предприятия, а также системных администраторов, имеющих прямой доступ к серверам, на которых хранятся персональные данные или их копии);

б) создание и утверждение четко определенного перечня персональных данных, подлежащих обработке; создание и утверждение документа «Описание системы защиты уязвимых персональных данных при их обработке в информационных системах обработки персональных данных в рамках предприятия». Заметим, что неотъемлемой частью вышеуказанного Описания должна стать Инструкция пользователя по соблюдению режима защиты информации при работе в информационных системах по обработке уязвимых персональных данных, а также Инструкция по резервному копированию и восстановлению данных в имеющихся информационных системах предприятия.

10. В соответствии с п. 2.1 Порядка от 08.01.2014 года №1/02-14, а также Законом Украины «О защите персональных данных» уведомить Уполномоченного Верховной Рады Украины по правам человека об обработке уязвимых персональных данных на предприятии.

Выводы. Стоит отметить, что уже сегодня биометрическая технология доказала свою эффективность и безопасность в широком ряду применения. Прогресс в области информационных технологий, в частности в сфере разработки и внедрения программного обеспечения, активность в формировании баз персональных данных чрезвычайно обострили проблему защиты частной жизни лица и целесообразности использования таких данных в ежедневной работе хозяйствующих субъектов. Мы убеждены, что в будущем биометрия в деятельности субъектов хозяйствования обеспечит оперативность в обработке персональных данных, оптимизирует ключевые процессы в администрировании работы на предприятии путем изменения паролей и электронных ключей для доступа не только к компьютерным программам, таких как «клиент – банк», но и к объектам, требующим усиленной защиты доступа, включая центры обработки данных или электронные биржевые системы.

Список использованной литературы:

1. LinkedIn подтвердила утечку свыше 100 млн. паролей пользователей // NEWSRU.com от 19.05.2016 г. [Электронный ресурс]. – Режим доступа : http://rus.delfi.lv/techlife/novosti/linkedin-podtverdila-utechku-svyshe-100-mln-parolej-polzovatelej.d?id=47459877.

2. Ризак М.В. Международное сотрудничество, связанное с оборотом и обработкой персональных данных с привлечением иностранных третьих лиц (иностранными субъектами отношений обращения и обработки персональных данных) / М.В. Ризак // Visegrad Journal of Human Rights № 4/2. – 2015. – С. 85.

3. Биометрические технологии для учета рабочего времени и управления персоналом [Электронный ресурс]. – Режим доступа : http://www.techportal.ru/glossary/uchet_rabochego_vremeni.html#.

4. Мировой рынок биометрической идентификации по лицу достигнет 24% к 2020 г. [Электронный ресурс]. – Режим доступа : http://www.plusworld.ru/daily/mirovoy-rinok-biometricheskoy-identifikacii-po-licu-dostignet-24-k-2020-g/.

5. Різак М.В. Особливості правового регулювання безпеки обігу «вразливих» персональних даних в Україні / М.В. Різак // Наукові записки Інституту законодавства Верховної Ради України. – 2012. – № 2. – С. 54.

6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 року // Офіційний вісник України від 14.01.2011 р., № 1; № 58, 2010, ст. 1994; стор. 701, стаття 85.

7. Про захист персональних даних : Закон України // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.

8. Правила участі в програмі «Оранж кард» [Электронный ресурс]. – Режим

доступа : http://www.orangecard.com.ua/ORANG_CARD_PCG_WWW_2_ru.pdf.

9. Политика ООО «Американ Экспресс Банк» в отношении обработки персональных данных [Электронный ресурс]. – Режим доступа : https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjIo8bD0sDNAhWJdCwKHfZ9Av0QFggdMAA&url=https%3A%2F%2Fbusiness.americanexpress.com%2Fru%2F~%2Fmedia%2FFiles%2FGCP%2Fru%2FPersonal_Data%2520Policy_AMEX_GCP_Russia.pdf&usg=AFQjCNHgY96_AYxCGNirLgapEh8HXnPTPg.

10. Кодекс поведінки при роботі з персональними даними у ПрАТ «Київстар» [Электронный ресурс]. – Режим доступа : https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwiNpqCU08DNAhVLGCwKHaJ1CPIQFggmMAM&url=http%3A%2F%2Fwww.kyivstar.ua%2Ff%2F1%2Fabout%2Fimportant_data%2Fcodex%2FCodex_Personal_Data.pdf&usg=AFQjCNEzRYaCnMhiBPXRhxa-tCpWWapBLA.

11. Положение о защите персональных данных в АО «БАЙЕР» [Электронный ресурс]. – Режим доступа : https://www.bayer.ru/privacy-statement.php.

12. Положение «О защите персональных данных» АО «Арселор Миттал Темиртау» [Электронный ресурс]. – Режим доступа : https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjklKuWwc3NAhUHWCwKHfpWAeQQFggaMAA&url=http%3A%2F%2Fwww.arcelormittal.kz%2Fpolicies%2Fcompliance.pdf&usg=AFQjCNHXClv2WLYlCLJh5PRmPUcI6DPPng.

13. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 // Бізнес-Бухгалтерія-Право. Податки. Консультації від 03.03.2014 р. – № 9. – С. 14.

О РОЛИ СУДА В СОСТЯЗАНИИ СТОРОН УГОЛОВНОГО ПРОЦЕССА

Юрий МИРОШНИЧЕНКО,
кандидат юридических наук, доцент кафедры конституционного, административного и международного права
Мариупольского государственного университета

Summary

Based on active legislation of Ukraine and theoretic material analyzed the author of the article concludes that evidentiary activity of the court should be of a subsidiary nature. This is needed when the parties fail, do not know how or simply do not want to exercise their rights and authority. Taking the initiative in this case, the court does not accuse or defend as well as does not give the precedence to any party. Its activity is aimed at determining the truth in criminal procedure in order to make fair and rationale judgement. To do so, the court has a set of procedural mechanisms analyzed in this particular research.

Key words: criminal procedure, competition, evidentiary activity of the court.

Аннотация

На основе анализа теоретического материала и действующего украинского законодательства автор статьи приходит к выводу о том, что доказательственная активность суда должна иметь субсидиарный характер. Такая необходимость может возникнуть тогда, когда стороны не могут, не умеют или не хотят использовать свои возможности и права. Проявляя в подобных ситуациях инициативу, суд не берет на себя выполнение функций обвинения или защиты и не стремится отдать предпочтение одной из сторон. Его активность направлена на установление истины в уголовном производстве для вынесения законного и обоснованного судебного решения. Для этого суд наделен соответствующим процессуальным инструментарием, который приводится в выводах данного исследования.

Ключевые слова: уголовный процесс, состязательность, доказательственная деятельность суда.

Постановка проблемы и актуальность темы исследования. Неотъемлемым элементом современного демократического правового государства является независимый и беспристрастный суд, деятельность которого основывается на состязательности сторон, свободе в представлении ими доказательств и отстаивании их убедительности перед судом. Среди ученых-юристов давно ведутся дискуссии по поводу содержательной характеристики состязательности и роли суда в состязательном процессе. В разные годы в той или иной степени эта тема исследовалась в работах Л.Ю. Ароцкера, К.К. Арсеньєва, В.И. Боярова, В.В. Вапнярчука, С.И. Викторского, Л.В. Головко, М.В. Духовского, О.В. Каплиной, С.Л. Кисленко, Л.М. Лобойко, П.А. Лупинской, В.Т. Маляренко, И.В. Михайловского, В.Т. Нора, Ю.К. Орлова, И.Д. Перлова, О.В. Пиюк, Н. Н. Полянського, Р.Д. Рахунова, А.Л. Ривлина, Н.П. Сизой, О.Б. Семухиной, В.К. Случевского, М.С. Строговича, И.Я. Фойницкого, А.А. Хмырова, А.Л. Цыпкина, Л.М. Шифмана, О.Г. Яновской и других представителей наук уголовного процесса и криминалистики. Однако, несмотря на значительный массив исследований отечественных и зарубежных правоведов, указанная проблема на фоне ломки уголовно-процессуальных парадигм, происходящей в течение последних десятилетий на постсоветском пространстве под влиянием изменения ценностных приоритетов и целых социальных систем, остается весьма актуальной.

Цель статьи. Действующий уголовный процессуальный кодекс Украины (далее – УПК) закрепил, что состязательность процесса предполагает: 1) самостоятельность сторон в отстаивании своих правовых позиций, прав, свобод и законных интересов; 2) равноправие сторон по сбору и представлению в суд доказательств, ходатайств, жалоб, а также по реализации других процессуальных прав; 3) распределение функций государственного обвинения, защиты и судебного рассмотрения, запрет на их совмещения. При этом, по тексту закона, суд, сохраняя объектив-