УДК 342.95

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ ПУБЛИЧНОЙ АДМИНИСТРАЦИИ В УКРАИНЕ

Анна БЛИНОВА,
кандидат юридических наук, доцент,
заведующий кафедрой гражданско-правовых дисциплин
Высшего учебного частного заведения
«Днепровский гуманитарный университет»

АННОТАЦИЯ

В статье проанализированы научные концепции понятия «информационная безопасность», определены его общие признаки, рассмотрены особенности информационной безопасности органов публичной администрации, сформулировано соответствующее авторское понятие и определены перспективы его легитимации.

Ключевые слова: органы публичной администрации, информационная безопасность, информационные отношения, информационная среда, угрозы информационной безопасности.

INFORMATION SECURITY OF BODIES OF PUBLIC ADMINISTRATION IN UKRAINE

Anna BLINOVA,
Candidate of Law Sciences, Associate Professor,
Head of the Department of Civil Disciplines, Law Faculty
Private Institution of Higher Education
"Dnipro University of the Humanities"

SUMMARY

The article analyzes the scientific views of the concept of "information security", defines its common features, discusses the features of information security of public administration bodies, formulates the corresponding author's concept and identifies prospects for its legitimization.

Key words: public administration authorities, information security, information relations, information environment, information security threats.

Постановка проблемы. Одной из гарантий эффективности информационного обеспечения органов публичной администрации является их информационная безопасность. Конституция Украины обеспечение информационной безопасности относит к важнейшим функциям государства. Концепция развития электронного управления в Украине определила недостаточный уровень информационной безопасности и защиты информации в информационно-телекоммуникационных системах органов власти одной из первоочередных проблем, которая демонстрирует значительное отставание Украины от мировых темпов развития электронного управления и такой, что требует совершенствования государственной политики в этой сфере, направленной на ее первоочередное решение [21]. Концепция развития цифровой экономики и общества Украины на 2018–2020 годы закрепляет седьмым принципом цифровизации – повышение уровня доверия и безопасности, который означает, что информационная безопасность, кибербезопасность, защита персональных данных, неприкосновенность личной жизни и прав пользователей цифровых технологий, укрепление и защита доверия в киберпространстве являются предпосылками одновременного цифрового развития и соответствующего предупреждения, устранения и управления сопутствующими рисками [22].

Особенно остро вопрос информационной безопасности встал во время сегодняшней военной агрессии, развязанной против Украины, что обнаружила комплекс угроз длительного характера. Военная доктрина Украины признает, что современным военным конфликтам присущи черты роли информационных средств при подготовке и в реализации военных мер. Военная доктрина Украины определяет одним из основных путей предотвращения возникновения военных конфликтов обеспечение информационной безопасности [18].

С 1995 года в Украине постоянно увеличивается количество деструктивных инцидентов, связанных с причинением вреда системам информационного обеспечения органов публичной администрации [5, с. 33]. Вследствие последней массовой кибератаки, которая состоялась летом 2017, была заблокирована деятельность таких предприятий, как аэропорт «Борисполь», «Укртелеком», «Укрпочта», «Ощадбанк», «Укрзалізниця» и ряда других крупных предприятий, заражению подверглись информационные системы Министерства инфраструктуры, Кабинета Министров, сайты Львовского городского совета, Киевской городской государственной администрации, киберполиции, Службы спецсвязи Украины и другие [26]. Вследствие этих событий Украина понесла значительный материальный ущерб, а общество было морально дестабилизировано. Приведенные факты свидетельствуют о том, что обеспечение информационной безопасности государства и органов публичной администрации, как ее подсистемы, являются современными

первоочередными задачами, которые требуют научного исследования.

Цель и задачи статьи. В связи с указанным целью статьи является определение основных признаков понятия «информационная безопасность», выяснения его содержания на основе анализа нормативно-правовых актов, существующих научных концепций и формулирование авторского определения информационной безопасности органов публичной администрации, а также определение перспектив его нормативного закрепления.

Состояние исследования. Содержание понятия «информационная безопасность» и особенности информационной безопасности различных субъектов исследовали такие ученые, как: В.Н. Богуш, И.Л. Близнюк, В.Л. Бурячок, В.Н. Желиховский, Б.А. Кормич, М.Б. Левицкая, В.А. Липкан, А.В. Логинов, Ю.Е. Максименко, А.В. Олейник, А.К. Юдин и другие. Однако отдельного научного изучения содержания понятия «информационная безопасность органов публичной администрации» не проводилось.

Изложение основного материала. Закон Украины «Об основах национальной безопасности Украины» определяет информационную безопасность составной частью национальной безопасности [20]. Доктрина информационной безопасности Украины определяет информационную безопасность как неотъемлемую составляющую каждой из сфер национальной безопасности и одновременно важную самостоятельную сферу обеспечения национальной безопасности. Именно поэтому развитие Украины как суверенного, демократического, правового и экономически стабильного государства возможен только при условии обеспечения надлежащего уровня его информационной безопасности [19]. В Законопроекте «Об информационном суверенитете и информационной безопасности» (ст. 3) информационная безопасность Украины определяется как защищенность жизненно важных интересов личности, общества и государства, при которой исключается причинение им вреда из-за неполноты, несвоевременности и недостоверности информации, при негативных последствиях функционирования информационных технологий или в результате распространения информации, запрещенной или ограниченной к распространению законами Украины [24]. В Законопроекте «Об основах информационной безопасности Украины» информационная безопасность определена как состояние защищенности жизненно важных интересов человека и гражданина, общества и государства, при котором предотвращается нанесение ущерба из-за неполноты, несвоевременности и недостоверности распространяемой информации, нарушение целостности и доступности информации, несанкционированный оборот информации с ограниченным доступом, а также из-за негативного информационно-психологического воздействия и умышленного причинения негативных последствий применения информационных технологий [23]. Действующее законодательство Украины не содержит определения понятия «информационная безопасность», не определяет его систему и виды.

В тоже время увеличение объемов информационных отношений в публичной сфере за последнее десятилетие, а также декларативные положения указанных выше нормативно-правовых актов о необходимости повышения уровня информационной безопасности Украины побудили научную общину активизировать исследования в этом направлении. Это привело к возникновению значительного количества научных концепций и подходов к пониманию понятия «информационная безопасность».

Результаты исследования информационной безопасности различных субъектов и процессов отражены в авторских определениях этого понятия. Так, Б.А. Кормич, исследуя различные научные концепции, отмечает, что распространенной является научная позиция, согласно которой информационная безопасность – это такое состояние защищенности жизненно важных интересов личности, общества и государства, при котором сводится к минимуму нанесение ущерба через неполноту, несвоевременность и недостоверность информации или отрицательного информационного воздействия через негативные последствия функционирования информационных технологий, а также из-за несанкционированного распространения информации [10, с. 77; 1, с. 73].

А.В. Олейник определяет информационную безопасность как осуществление комплекса системных превентивных мер по предоставлению гарантий защиты от негативных информационных воздействий: жизненно важных интересов личности, общества, государства; политического, экономического, научно-технологического, гуманитарного, социокультурного развития, поддержания обороны, государственной и экологической безопасности, системы государственного управления на необходимом уровне; обеспечение информационного суверенитета и безопасного развития национального информационного пространства; от манипулирования информацией, дезинформации и влияния на сознание, подсознание и психику индивида, общественных групп, общества в целом; своевременность и адекватность мер противодействия и нейтрализации всего спектра негативных факторов опасности, которые могут быть применены против Украины [17]. По мнению М.М. Галамба, понятие информационной безопасности государства следует также рассматривать в контексте обеспечения безопасных условий существования информационных технологий, включающих вопросы защиты информации как таковой, информационной инфраструктуры государства, информационного рынка и создание безопасных условий существования и развития информационных процессов. Этот ученый считает, что необходимый уровень информационной безопасности обеспечивается совокупностью политических, экономических, организационных мероприятий, направленных на предупреждение, выявление и нейтрализацию тех обстоятельств, факторов и действий, которые могут причинить ущерб или повредить реализации информационных прав, потребностей и интересов страны и ее граждан [6]. В.М. Торяник считает, что по своему содержанию информационная безопасность Украины является важной составляющей национальной безопасности, которая понимается как состояние защищенности информационного пространства, обеспечивая его формирование и развитие в интересах граждан, организаций

и государства в целом, защита от неправомерного внешнего и внутреннего вмешательства [25].

Наиболее умеренной относительно содержания понятия «информационная безопасность», по мнению Б.А. Кормич, кажется общая позиция стран-членов Европейского Союза, которую высказал представитель Швеции при обсуждении вопросов международной информационной безопасности на 56-й сессии Генеральной Ассамблеи ООН: «Информационная и сетевая безопасность – это защита личной информации отправителей и получателей, защита информации от несанкционированных изменений, защита от несанкционированного доступа к информации и создание надежного источника поставок оборудования, услуг и информации» [8, с. 41]. Сам же Б.А. Кормич определил информационную безопасность: как состояние защищенности установленных законодательством норм и параметров информационных процессов и отношений, которая обеспечивает необходимые условия существования государства, человека и общества как субъектов этих процессов и отношений [9, с. 78]. А.К. Юдин и В.М. Богуш определяют информационную безопасность: как состояние защищенности информационной среды общества, что обеспечивает его формирование, использование и развитие в интересах граждан, организаций, государства [27, с. 38]. Под информационной средой они понимают сферу деятельности субъектов, связанную с созданием, преобразованием и потреблением информации.

Все эти определения свидетельствуют о том, отмечает А.В. Логинов, что информационная безопасность выступает как признак стабильного, устойчивого состояния системы органов исполнительной власти, при воздействии внутренних и внешних угроз и опасностей, которая сохраняет существенно важные характеристики для собственного существования [13, с. 12]. Однако, по мнению А.В. Логинова, рассматривать безопасность только как состояние не совсем уместно. Она должна учитывать будущее, следовательно, является не состоянием, а процессом. Таким образом, информационную безопасность следует рассматривать сквозь органическое единство таких признаков, как состояние, свойство, а также управление угрозами и опасностями, с помощью которого обеспечивается избрание оптимального пути их устранения и минимизации влияния негативных последствий [13, с. 12]. По мнению И.А. Громыко и Т.И. Саханчука, информационная безопасность Украины – это защищенность государственных интересов, при которой обеспечивается предотвращение, выявление и нейтрализация внутренних и внешних информационных угроз, сохранение информационного суверенитета государства и безопасное развитие международного информационного сотрудничества [7]. На сегодня наиболее основательно исследованы подходы к определению информационной безопасности такими учеными, как: В.А. Липкан, Ю.Е. Максименко, В.М. Желиховская [12, с. 25–35], А.В. Логинов [14, с. 272]. Анализ приведенных определений позволяет выявить отсутствие единодушия ученых относительно признаков информационной безопасности, однако прослеживается тенденция к пониманию этого явления как определенного состояния безопасности в информационной сфере.

Определить объекты защиты, его механизм и цели позволит формулировка признаков информационной безопасности. Так, для информационной безопасности характерны следующие признаки: 1) по содержанию это состояние защищенности жизненно важных интересов человека и гражданина, личности, общества и государства; установленных законодательством норм и параметров информационных процессов и отношений; информационной среды общества; государственных интересов, а также свойства и управления угрозами и опасностями, с помощью которого обеспечивается избрание оптимального пути их устранения и минимизации влияния негативных последствий; 2) объектами защиты являются жизненно важные интересы личности, общества и государства в сфере политического, экономического, научно-технологического, гуманитарного, социокультурного развития, обороны, безопасности, государственного управления, информационного суверенитета и безопасного развития национального информационного пространства, информационной инфраструктуры государства, информационного рынка и т.д.; 3) защита осуществляется от таких угроз, как: несанкционированный доступ к информации; распространение и использование неполной, несвоевременной, недостоверной информации; нарушение целостности и доступности информации; манипулирования информацией, дезинформации; несанкционированный оборот информации с ограниченным доступом; распространение информации, запрещенной или ограниченной к распространению законами Украины; отрицательное информационно-психологическое воздействие на сознание, подсознание и психику индивида, общественных групп, общества в целом; 4) механизм достижения такого состояния предусматривает осуществление комплекса системных превентивных мер по предоставлению гарантий защиты объектов от негативных информационных воздействий; своевременность и адекватность мер противодействия и нейтрализации всего спектра негативных опасных факторов; создание безопасных условий существования и развития информационных процессов; комплекс политических, экономических, организационных, правовых мероприятий, направленных на предупреждение, выявление и нейтрализацию тех обстоятельств, факторов и действий, которые могут причинить ущерб или повредить реализации информационных прав, потребностей и интересов страны и ее граждан; 5) целью установления такого состояния безопасности является создание необходимых условий существования государства, человека и общества как субъектов информационных процессов и отношений; обеспечение формирования информационной среды общества, использование и развитие его в интересах граждан, организаций, государства; создание надежных источников телекоммуникационного оборудования, электронных, цифровых услуг и информации; предотвращение, выявление и нейтрализация внутренних и внешних информационных угроз; исключения или сведения к минимуму нанесения ущерба через реализацию внутренних или внешних угроз; сохранение информационного суверенитета государства и безопасное развитие международного информационного сотрудничества.

Приведенные признаки информационной безопасности отражают

особенности ее видов, которые могут быть определены по различным критериям. Например, в ч. 3 ст. 5 Закона Украины «Об основах национальной безопасности» законодатель связывает информационную безопасность с различными видами объектов: человеком, обществом и государством [20]. Ссылаясь на это положение, Б.А. Кормич выделяет три вида информационной безопасности: информационная безопасность человека, информационная безопасность общества, информационная безопасность государства [8, с. 40]. А.К. Юдин, В.М. Богуш, М.Б. Левицкая поддерживают это разделение информационной безопасности на виды по критерию объекта [11, с. 9]. Однако А.К. Юдин и В.М. Богуш, признавая существование информационной безопасности государства и общества, объединяют и отождествляют их. В своей монографии они отмечают, что информационная безопасность государства (общества) характеризуется степенью защищенности государства (общества) и устойчивости основных сфер жизнедеятельности (экономики, науки, техносферы, сферы управления, военного дела и т.д.) относительно опасных (дестабилизирующих, деструктивных, поражающих государственные интересы и т.д.) информационных воздействий, причем как по внедрению, так и извлечению информации. Единственное, чем отличаются эти два вида информационной безопасности, по их мнению, это тем, что информационная безопасность государства определяется способностью нейтрализовать такие воздействия [27, с. 41]. М.Б. Левицкая рассматривает также национальную безопасность, которую определяет: как такую степень защищенности личности, государства и общества, которая обеспечивает их устойчивое функционирование и базируется на деятельности людей, государства, общества и мирового сообщества для выявления, предупреждения, пресечения и ликвидации последствий угроз национальным интересам [11, с. 7]. Этот же вид безопасности Б.А. Кормич определяет: как состояние защищенности гарантированных законодательством условий жизнедеятельности государства, общества и отдельной личности от внутренних и внешних угроз [10, с. 14-15]. По мнению А.В. Логинова, информационная безопасность – это состояние управления национальными интересами, угрозами и опасностями в сфере информационных отношений, при котором подсистема информационной безопасности максимально долго не будет превышать пороговых параметров своего функционирования [15, с. 202]. С ускорением процессов глобализации и международного сотрудничества, на наш взгляд, существует актуальная необходимость выделить высший уровень информационной безопасности – международную информационную безопасность, где объектами будут интересы международных, межгосударственных и межправительственных организаций. На этой позиции находится также И.Л. Близнюк, который отмечает, что система информационной безопасности является одновременно и элементом в системе высшего уровня – международного, национального, местного [2, с. 208].

Приведенные выше научные концепции не определяют такие виды информационной безопасности, как информационная безопасность отрасли, ведомства, учреждения, организации, предприятия, органов местного самоуправления, территориальной общины. Эти виды, на наш взгляд, являются ключевыми звеньями в формировании отечественной системы информационной безопасности государства. Таким образом, мы считаем, что система информационной безопасности может быть следующих видов: 1) международная информационная безопасность; 2) государственная информационная безопасность; 3) информационная безопасность общества; 4) информационная безопасность территориальной общины 5) информационная безопасность органов местного самоуправления; 6) информационная безопасность отрасли общественного производства; 7) информационная безопасность ведомства (министерства), органа государственной власти; 8) информационная безопасность учреждения, организации, предприятия; 9) информационная безопасность человека, гражданина, личности [16, с. 159–160]. С учетом растущего числа несанкционированного доступа к информационным ресурсам органов публичной администрации, государственных информационно-телекоммуникационных систем, совершения незаконных действий с информацией в государственных базах данных злоумышленниками наносится значительный материальный ущерб государству, предприятиям, учреждениям, организациям и физическим лицам, а также дестабилизируется общество. Повысить уровень информационной безопасности государства и общества в целом позволит разработка и внедрение концепции информационной безопасности органов публичной администрации, которая должна учесть результаты передовых научных исследований и согласовываться с другими концепциями, доктринами, планами в сфере регулирования информационных отношений.

Выводы. С учетом понятия органов публичной администрации, их информационных потребностей и интересов, которые были определены нами в предыдущих научных работах [3; 4], а также с убеждением, что в сфере информационных отношений существование состояний невозможно либо краткосрочно, что обусловлено самим содержанием информации и развитием информационных технологий, считаем возможным выделить следующие признаки информационной безопасности органов публичной администрации: 1) по содержанию это процесс достижения состояния защищенности; 2) объектами защиты являются интересы органов публичной администрации, их информационная среда, информационные отношения, информационная инфраструктура и связанные с ними технологические объекты и инфраструктура; 3) защита осуществляется от таких угроз, как: несанкционированный доступ к информации; распространение и использование неполной, несвоевременной, недостоверной информации; нарушение целостности и доступности информации; манипулирования информацией, дезинформации; несанкционированный оборот информации с ограниченным доступом; распространение информации, запрещенной или ограниченной к распространению законами Украины; негативное информационное влияние на репутацию органов публичной администрации и сознание их работников; 4) механизм достижения такого состояния предусматривает осуществление комплекса системных превентивных мер по предоставлению гарантий защиты объектов от негативных информационных воздействий; своевременность

и адекватность мер противодействия и нейтрализации всего спектра негативных опасных факторов; создание безопасных условий существования и развития информационных процессов; комплекс организационных мероприятий, направленных на предупреждение, выявление и нейтрализацию тех обстоятельств, факторов и действий, которые могут нанести ущерб или повредить реализации информационных потребностей и интересов органов публичной администрации; 5) целью и задачами установления такого состояния безопасности является создание необходимых условий эффективного функционирования органов публичной администрации как субъектов информационных отношений; обеспечение формирования их безопасной информационной среды, использования ее в интересах граждан общества и государства; создание надежных источников и обслуживание телекоммуникационного оборудования органов публичной администрации, электронных, цифровых услуг и информации; предотвращение, выявление и нейтрализация внутренних и внешних информационных угроз; исключения или сведения к минимуму нанесенного ущерба через реализацию внутренних или внешних угроз; сохранение информационной самостоятельности органов публичной администрации в рамках информационного суверенитета государства; безопасное развитие международного информационного сотрудничества органов публичной администрации.

Таким образом, опираясь на ключевые признаки информационной безопасности органов публичной администрации, ее можно определить как процесс реализации комплекса системных превентивных, охранных, защитных, организационных, правовых, технических мероприятий, направленных на обеспечение состояния защищенности информационных интересов органов публичной администрации, их информационных отношений, среды и инфраструктуры, от внутренних и внешних негативных факторов с целью создания необходимых условий для эффективного функционирования органов публичной администрации.

Этим определением, на наш взгляд, должны быть дополнены проекты Информационного кодекса Украины, законов Украины «Об основах информационной безопасности Украины», «Об информационном суверенитете и информационной безопасности Украины», «Об информационном обеспечении органов публичной администрации». В последнем нормативно-правовом акте предлагаем в отдельном разделе детально определить принципы, систему, механизм и его элементы, субъекты обеспечения информационной безопасности органов публичной администрации и их полномочия. Указанные предложения требуют дальнейшего научного исследования в следующих работах.

Список использованной литературы:

1. Баранов А. Информационный суверенитет или информационная безопасность? Національна безпека і оборона. 2001. № 1. С. 70–76.
2. Близнюк І.Л. Інформаційна безпека України та заходи її забезпечення. Наук. вісник Нац. акад. внутр. справ України. 2003. № 5. С. 206–214.
3. Блінова Г.О. Органи публічної адміністрації як суб'єкти інформаційних відносин. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. № 1. 2018. С. 144–150.
4. Блінова Г.О. Поняття, зміст та види інформаційних потреб та інтересів органів публічної адміністрації. Актуальні проблеми вітчизняної юриспруденції. № 5. 2018. С. 55–58.
5. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. К.: ДУТ, 2015. 288 с.
6. Галамба М. Інформаційна безпека України: поняття, сутність та загрози. / М. Галамба, В. Петрик. Юридичний журнал. URL: http://www.justinian.com.ua/article.php?id=2463
7. Громико І., Саханчук Т., Зінов'єв О. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. Право України. 2008. № 8. С. 130–134.
8. Кормич Б.А. Класифікація видів інформаційної безпеки. Митна справа. 2004. № 5. С. 40–48.
9. Кормич Б.А. Компетенція держави у сфері інформаційної безпеки. Митна справа. 2005. № 1. С. 76–82.
10. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук: 12.00.07; Нац. ун-т внутр. справ. Х., 2004. 42 с.
11. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.01; НАН України; Ін-т держави і права ім. В.М. Корецького. К., 2002. 17 с.
12. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. К.: КНТ, 2006. 280 с.
13. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: автореф. дис. ... канд. юрид. наук: 12.00.07; Нац. акад. внутр. справ України. К., 2005. 20 с.
14. Логінов О.В. Загрози національним інтересам особистості в інформаційній сфері України. Наук. вісн. Юрид. акад. М-ва внутр. справ. 2004. № 3. С. 271–275.
15. Логінов О.В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління. Наук. вісн. Юрид. акад. М-ва внутр. справ. 2003. № 3. С. 199–205.
16. Макушев П.В., Блінова Г.О. Розголошення відомостей військового характеру як загроза національній безпеці України. Військові злочини: кримінально-правова, криміналістична та кримінологічна характеристика: монографія. Херсонський національний університет. Херсон. 2015 р. С. 150–172.
17. Олійник О.В. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. Наукові записки Інституту законодавства Верховної Ради України. 2015. № 1. С. 54–59. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2015_1_15
18. Про Воєнну доктрину України: Указ Президента України від 15 червня 2004 року № 648/2004. Президентський вісник від 23.06.2004 № 14.
19. Про Доктрину інформаційної безпеки України: Указ Президента України від 8 липня 2009 року № 514/2009. URL: http://zakon4.rada.gov.ua/laws/show/514/2009

20.Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964-IV. Офіційний вісник України. № 29. Ст. 1433.

21.Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р. Урядовий кур'єр від 27.09.2017. № 181.

22.Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Урядовий кур'єр від 11.05.2018. № 88.

23.Проект Закону «Про засади інформаційної безпеки України» № 4949 від 28.05.2014 вноситься народними депутатами України І.М. Стойком, О.І. Кузьмуком, Ю.М. Сиротюком. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123

24.Проект Закону України «Про інформаційний суверенітет та інформаційну безпеку України» від 12.08.99 р. Вносить народний депутат України Чиж І.С. (в.о. 190). Текст № 1207.

25. Торяник В.М. Інформаційна безпека як складова національної безпеки Держави. Роль ЗМІ у забезпеченні інформаційного суверенітету України. Право і суспільство. № 2. 2016. С. 151–155.

26.Хакерська атака на Україну: подробиці. URL: https://www.rbc.ua/ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html

27.Юдін О.К., Богуш В.М. Інформаційна безпека держави: навч. посіб. Х.: Консум, 2005. 576 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Блинова Анна Александровна – кандидат юридических наук, доцент, заведующий кафедрой гражданско-правовых дисциплин Высшего учебного частного заведения «Днепровский гуманитарный университет»

INFORMATION ABOUT THE AUTHOR

Blinova Anna Aleksandrovna – Candidate of Law Sciences, Associate Professor, Head of the Department of Civil Disciplines, Law Faculty Private Institution of Higher Education "Dnipro University of the Humanities"

uk_dgu@ua.fm

УДК 343.13

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЧАСТНИКОВ УГОЛОВНОГО ПРОЦЕССА В УКРАИНЕ

Алексей БОЙКО,
кандидат юридических наук,
преподаватель кафедры уголовного процесса
Днепропетровского государственного университета внутренних дел

Валерий ЛИТВИНОВ,
кандидат юридических наук,
доцент кафедры уголовного процесса
Днепропетровского государственного университета внутренних дел

АННОТАЦИЯ

Статья освещает проблемы обеспечения безопасности участников уголовного процесса Украины. Авторами затронут вопрос о необходимости закрепления в Уголовном процессуальном кодексе Украины (далее – УПК Украины) отдельной главы, которой будут урегулированы основания и процессуальный порядок применения мер обеспечения безопасности участников уголовного процесса. Указано на необходимость предусмотреть в УПК Украины обязанность следователя, прокурора, следственного судьи, суда принимать меры по обеспечению безопасности участников уголовного процесса. С целью надлежащего обеспечения безопасности всех лиц, которые принимают участие в уголовном процессе, предложено расширить их перечень. На основе проведенного исследования авторами обоснована необходимость и пути совершенствования норм УПК Украины по обеспечению безопасности участников уголовного процесса.

Ключевые слова: следователь, прокурор, следственный судья, суд, меры безопасности, обеспечение безопасности, участники уголовного процесса, уголовное производство.

THE SECURITY CONSTRAINTS OF PARTICIPANTS IN THE CRIMINAL PROCESS OF UKRAINE

Aleksey BOYKO,
PhD in Law,
Lecturer at the Department of Criminal Proceeding
of Dnipropetrovsk State University of Internal Affairs

Valeriy LITVINOV,
PhD in Law,
Assistant Professor at the Department of Criminal Proceeding of Dnipropetrovsk State University of Internal Affairs

SUMMARY

The article deals with the security constraints of participants in the criminal process of Ukraine. The authors have raised the issue of the need to fix a separate chapter in the Criminal Procedure Code of Ukraine (hereinafter – the Code of Criminal Procedure of Ukraine), which will regulate the basis and procedure for the application of measures to ensure the security of participants in criminal proceedings. It is shown the necessary of providing in the Criminal Procedure Code of Ukraine the obligation to take measures ensuring the security of participants in criminal proceedings by the investigator, prosecutor, investigating judge and court. In order to properly ensuring the security of all persons who take part in the criminal process the idea of expanding their list is proposed. The study demonstrates a need and ways to improve the norms of the Criminal Procedure Code of Ukraine to ensure the security of participants in criminal proceedings.

Key words: investigator, prosecutor, investigating judge, court, measures of the security, ensuring the security, participants in criminal process, criminal proceeding.