



## ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЖИТЕЛЕЙ СЕЛЬСКОЙ МЕСТНОСТИ В УКРАИНЕ (ТЕЛЕКОММУНИКАЦИОННЫЙ АСПЕКТ)

Диана АНТИПЕНКО,

аспирант кафедры административного и финансового права  
Национального университета биоресурсов и природопользования Украины

### Summary

The research devoted to the comprehensive analysis of theoretical and methodological, organizational and legal bases of the ensuring of information security of villagers as consumers of telecommunications services in Ukraine. The essence of information and communication infrastructure of rural areas is researched. Also it is determined the system of subjects ensure to development this infrastructure in Ukraine. The significance of information and communication infrastructure of rural areas in the aspect of the transition to the priority scientific-technical and innovation development of Ukraine.

**Key words:** information society, ensuring of information security, consumers of telecommunications services, villagers, organizational and legal bases.

### Аннотация

Исследование посвящено комплексному анализу теоретико-методологических и организационно-правовых основ обеспечения информационной безопасности жителей сельской местности как потребителей телекоммуникационных услуг в Украине. Исследована сущность информационно-коммуникационной инфраструктуры сельской местности, определена система субъектов обеспечения её развития в Украине. Определена значимость информационно-коммуникационной инфраструктуры сельской местности в аспекте перехода к приоритетному научно-техническому и инновационному развитию Украины.

**Ключевые слова:** информационное общество, обеспечение информационной безопасности, потребители телекоммуникационных услуг, жители сельской местности, организационно-правовые основы.

**Цель и задача данной работы** состоят в комплексном исследовании теоретико-методологических и организационно-правовых основ обеспечения информационной безопасности жителей сельской местности как потребителей телекоммуникационных услуг в Украине.

**Методологическую основу исследования** составляют диалектический метод научного познания социально-правовых и социально-технических явлений и процессов, а также контент-анализ, сравнительно-правовой и некоторые другие научные методы, характерные для современных наук информационного и административного права.

**Изложение основного материала.** В реалиях информационного общества ключевую роль в развитии сельской местности (как в производственном, так и в социальном аспекте) играет современная информационно-коммуникационная инфраструктура. В свою очередь, процесс развития последней неразрывно связан с развитием современных телекоммуникаций. Как отмечают специалисты, общественное развитие последнего десятилетия демонстрирует беспрецедентную интенсификацию влияния телекоммуникаций (электросвязи) на мировой социум [1, с. 4; 2, с. 4]. Подтверждение особен-

ного «статуса» телекоммуникаций в современном глобализованном мире можно найти и в законодательстве Украины, и международно-правовых документах:

1) в «Концепции развития телекоммуникаций в Украине», утвержденной распоряжением Кабинета Министров Украины (далее – КМУ) от 07.06.2006 г. № 316, отмечается, что в соответствии с принципами построения глобальной информационной инфраструктуры, телекоммуникации являются составляющей, обеспечивающей свободное движение информации между ее многочисленными информационно-специализированными частями, такими как источники и потребители информации, хранилища и базы данных, переработчики и распространители информации и т.п. (раздел 4);

2) в Законе Украины «О телекоммуникациях» от 18.11.2003 г. отмечается, что они являются неотъемлемой частью производственной и социальной инфраструктуры страны и предназначены для удовлетворения потребностей физических и юридических лиц, органов государственной власти в телекоммуникационных услугах (ч. 2 ст. 3);

3) в так называемом «Женевском плане действий» [3] в контексте минимизации «цифрового» неравенства сельских районов акцентируется осо-

бое внимание на необходимости создания устойчиво функционирующих многоцелевых публичных пунктов коллективного доступа к различным ресурсам связи, в первую очередь Интернет. При этом подчеркивается, что именно основанные на телекоммуникациях продукты и услуги обеспечивают практически мгновенный доступ к информации и знаниям в любой точке планеты (п. 10).

Анализ показал, что указанные тенденции освещались во многих юридических работах. Среди них, прежде всего, следует отметить труды таких учёных, как И.В. Аристова, О.А. Баранов, И.Л. Бачило, К.И. Беляков, О.Г. Белорус, В.М. Брыжко, О.Г. Волеводз, Р.А. Каложный, В.О. Копылов, Б.А. Кормич, А.Г. Кузьменко, В.А. Липкан, А.В. Логинов, А.И. Марущак, В.Б. Рушайло, Г.В. Семенов, Ю.Г. Соколов, А.О. Стрельцов, В.С. Цимбалюк и многих других. Обобщение научных достижений этих ведущих специалистов в контексте тематики данной статьи позволяет прийти к выводу о том, что интенсивное развитие телекоммуникаций обуславливает не только положительные для бытия человека, общества и государства последствия, но и негативные. Именно поэтому следует выделить исследование Д.В. Сулацкого [2], в котором было проведено, в рамках наук



информационного и административно-го права, изучение телекоммуникационного аспекта информационной безопасности с учетом глобализационных процессов. При этом среди наиболее актуальных и злободневных угроз информационной безопасности человека автором охарактеризованы информационно-психологическое воздействие (влияние) индивидуальной и массовой направленности, киберпреступность (компьютерная преступность), в том числе перехват телекоммуникаций, а также ограничение доступа потребителей к телекоммуникационным услугам. Вместе с тем приходится признать фактическое отсутствие научных работ, освещающих указанную проблематику в аспекте сельской местности и ее жителей, что и обуславливает особую актуальность выбранной нами темы.

Для решения поставленной задачи, прежде всего, следует коротко охарактеризовать отдельные результаты наших предыдущих исследований по проблемам развития информационно-коммуникационной инфраструктуры сельской местности (далее – ИКИСМ), представляющих особенную важность для текущей работы. Речь идет об авторской концепции нового организационно-правового механизма обеспечения прав и свобод представителей аграрноориентированных территорий за счет использования ИКИСМ. Упомянутый механизм, прежде всего, нацелен на активную форму участия сельских жителей в отношениях и процессах, связанных с развитием и функционированием указанной инфраструктуры, а также учитывает модель организационно-правового механизма ее развития, составляющими элементами которого являются институциональное, правовое, организационное и ресурсное обеспечение.

В свою очередь, охарактеризованные в начале данной статьи негативные тенденции обуславливают вывод о том, что процесс развития ИКИСМ нуждается в обязательной корректировке с учетом обеспечения информационной безопасности. Более того, возникает объективная необходимость в комплексном исследовании указанной безопасности как с позиции самой ИКИСМ, так и с позиции потребителя телекоммуникационных услуг – сель-

ского жителя. Таким образом, и надлежащая реализация предложенной нами ранее концепции нового механизма невозможна без изучения организационно-правовых основ обеспечения информационной безопасности вышеупомянутых объектов, что и будет осуществлено в рамках данной работы.

Не вызывает сомнений тот факт, что выполнение поставленного задания предусматривает проведения детального доктринально-правового анализа феномена информационной безопасности и связанных с ним категорий. Прежде всего, отметим, что, по результатам обобщения соответствующей историографической базы, исследуемая безопасность выступает новым и довольно динамическим направлением современных знаний [1-8]. Поэтому в этой сфере нет четко сформулированной и, главное, общепризнанной терминологии.

Так, украинский ученый В.Д. Недиличенко выделяет два основных подхода к восприятию сущности информационной безопасности в Украине: 1) защита информации – то есть защищенность содержания сведений от деструктивного влияния (объектом защиты выступает информация); 2) безопасность информации – то есть защищенность общества и личности от деструктивного влияния содержания сведений (объект защиты – личность и общество). И уточняет, что эти понятия принципиально отличаются по цели. Если первым охватывается защита содержания сведений независимо от характера последних, то вторым, наоборот, предусматривается блокирование распространения сведений в зависимости от характера их содержания. При этом воздействие (угрозы) первого типа трактуется как технологическое и изучается специалистами по информатики и управлению. Воздействие второго типа определяется как гуманитарное и анализируется психологами, социологами, политологами, культурологами, философами, специалистами оборонной и других сфер [6, с. 90-91]. Следует добавить, что и юридическая наука, на наш взгляд, может внести существенный вклад в исследование второго подхода.

Отметим то, что оба приведенных подхода к определению сущности информационной безопасности являют-

ся актуальными по отношению как к ИКИСМ, так и к ее пользователям – жителям сельской местности. Для проверки указанной позиции обратимся к работе Ю.Е. Максименко, которая рассматривает информационную безопасность как систему, состоящую из следующих структурных элементов: 1) информационно-технической безопасности; 2) информационно-психологической безопасности; 3) информационной безопасности в сфере прав и свобод человека и гражданина [7, с. 10-11]. Вместе с тем, оперируя другими научными результатами [2; 4; 5; 8], можно заметить определенную релятивность предложенной системы, обусловленной тесными взаимозависимостью и взаимопроникновением выделенных элементов, вероятной перспективой расширения их перечня.

Таким образом, проведенное доктринальное исследование демонстрирует достаточно сложную и многогранную природу феномена информационной безопасности. Это обуславливает необходимость изучения также и норм действующего законодательства, регулирующих общественные отношения в данной сфере. Соответствующий анализ положений Конституции Украины от 28.06.1996 г. (ст. 17), законов Украины «О Национальной программе информатизации» от 04.02.1998 г. (ст. 5-6), «О Концепции Национальной программы информатизации» от 04.02.1998 г. (п. 3 раздел IV), «О телекоммуникациях» от 18.11.2003 г. (ч. 1 ст. 1), «Об основах национальной безопасности Украины» от 19.06.2003 г. (ст. 6-8), «О главных основах развития информационного общества в Украине на 2007-2015 годы» от 09.01.2007 г. (п. 13 раздел III), а также других нормативно-правовых актов свидетельствует о существовании несогласованности между действующими правовыми нормами в части определения сущности и понятия информационной безопасности. Более того, национальное законодательство существенно «отстает» от динамики изменений, обусловленных развитием информационного общества в Украине и мире. Поэтому многие элементы последнего существуют вне правового поля, не регулируются нормативно-правовыми актами, а это сдерживает его полноценное развитие. При этом значительная часть из разработан-



ных проектов актов несовершенна и некорректна с точки зрения действующего законодательства [9].

С нашей точки зрения, установлению причин сложившейся ситуации будет способствовать в значительной мере выяснение позиций органов государственной власти Украины относительно перспективного планирования их нормотворческой деятельности, а также современных украинских законодательских (нормотворческих) тенденций в сфере информационной безопасности, которые, прежде всего, связаны с обеспечением, так называемой, кибернетической безопасности (или же кибербезопасности) [5]. В связи с этим необходимо отметить:

1) указы Президента Украины: от 10.12.2010 г. № 1119 «О решении Совета национальной безопасности и обороны Украины от 17 ноября 2010 года «О вызовах и угрозах национальной безопасности Украины в 2011 году» (п. 4); от 08.06.2012 г. № 388 «О решении Совета национальной безопасности и обороны Украины от 25 мая 2012 года «О мероприятиях по усилению борьбы с терроризмом в Украине» (п. 1); от 08.06.2012 г. № 389 «О решении Совета национальной безопасности и обороны Украины от 8 июня 2012 года «О новой редакции Стратегии национальной безопасности Украины» (п.п. 3.1.1, 3.3, 4.3), от 08.06.2012 г. № 390 «О решении Совета национальной безопасности и обороны Украины от 8 июня 2012 года «О новой редакции Военной доктрины Украины» (п.п. 7, 19);

2) нормативно-правовые акты КМУ: Распоряжение от 22.08.2012 г. № 720-р «Об утверждении плана мероприятий по выполнению Годовой национальной программы сотрудничества Украина – НАТО на 2012 год», а также Поручение от 15.06.2012 г. № 24066/1/1-12 к вышеуказанному Решению Совета национальной безопасности и обороны Украины (далее – СНБО), введенного в действие Указом Президента Украины от 08.06.2012 г. № 388;

3) внесенный народным депутатом Украины А.Л. Деркачом проект Закона Украины «О внесении изменений в некоторые законы Украины относительно обеспечения кибернетической безопасности Украины» [10], соавтором которого выступает заместитель Секретаря СНБО В.Л. Сивкович. Указан-

ном законопроектом, среди прочего, предусмотрено введения в отечественное законодательство таких понятий, как «кибернетическая безопасность государства», «объекты критической инфраструктуры», «объекты критической информационной инфраструктуры» и т.п.;

4) подготовленный Государственной службой специальной связи и защиты информации Украины в рамках исполнения упомянутых решений СНБО и соответствующих поручений КМУ проект Закона Украины «Об основных принципах обеспечения кибернетической безопасности Украины», содержащем определение понятия «кибернетическая безопасность (кибербезопасность)», «Национальная критическая инфраструктура» и т.п. [11, с. 1-3];

5) разработанный Министерством внутренних дел Украины (далее – МВД) во исполнение Поручения КМУ от 15.06.2012 г. № 24066/1/1-12 к вышеуказанному Решению СНБО, по согласованию с КМУ (Поручение от 21.08.2012 г. № 24066/34/1-12 к письму МВД от 15.08.2012 г. № 12465/Рт) и СНБО (письмо от 23.08.2012 г. № 1621/3-11-4 в адрес МВД) проект Закона Украины «О внесении изменений в Закон Украины «Об основах национальной безопасности Украины» (относительно кибернетической безопасности Украины)» [12]. Проект указанного Закона определяет основные угрозы национальной безопасности кибернетического характера, основные направления государственной политики и основные функции субъектов обеспечения национальной безопасности в этой сфере, а также содержит определение понятий «кибернетическая безопасность (кибербезопасность)», «кибернетическое пространство (киберпространство)». Нужно выделить и то обстоятельство, что в законопроекте МВД впервые учтены соответствующие позиции Министерства обороны, Министерства юстиции, Службы безопасности, Службы внешней разведки, Государственной службы специальной связи и защиты информации Украины, а также других заинтересованных органов.

Завершая на этом рассмотрение украинских законодательских тенденций относительно разрешения связанных с вопросами кибербезопасности,

можно выделить две группы тенденций и факторов:

1) положительные, с точки зрения усовершенствования нормативно-правового обеспечения кибернетической безопасности Украины, выступающей неотъемлемой составляющей информационной безопасности государства. Они связаны с необходимостью осознания национальной провластной элитой острой необходимости в принятии законодательных новаций в этой сфере, а также активным поиском соответствующими центральными органами исполнительной власти оптимальных путей решения данной проблемы;

2) негативные, прежде всего, в организационном и институциональном аспектах. Анализ источников указывает на отсутствие системного подхода к решению законодательных проблем в сфере безопасности. Это проявляется в несогласованности действий различных государственных учреждений, а также в несогласованности принятых управленческих решений. Типичным примером этого может выступать ситуация с одновременным определением нескольких основных исполнителей одной и той же задачи по разработке законопроекта о кибербезопасности. Добавим и то, что проблемы такого характера свойственны практически всем сферам общественной жизни Украины, в том числе и аграрной сфере.

Одновременно можно сделать и еще один важный вывод, который расширяет границы понимания сущности информационной безопасности сельских жителей как потребителей телекоммуникационных услуг. Природно-климатический (природно-ресурсный) и трудовой потенциал Украины, исторически обусловленная социальная значимость аграрного сектора для ее сообщества, а также обострение глобального продовольственного кризиса обуславливают необходимость определения ИКИСМ в качестве одного из основных объектов кибернетической защиты государства [13, с. 89; 14, с. 33]. С нашей точки зрения, это необходимо учитывать в процессе проектирования, как Национальной системы кибернетической безопасности, так и самой ИКИСМ. Очевидно, что предложенные организационно-правовые меры будут значительно способствовать обеспечению информационной безопасности



сельских жителей как потребителей телекоммуникационных услуг.

Важно выделить и тот факт, что в условиях информационного общества от надлежащего, безопасного функционирования ИКИСМ будет зависеть и качественное, безопасное обеспечение личных (гражданских), политических, социальных, экономических, культурных, экологических и других прав и свобод сельских жителей. В связи с этим целесообразно вновь упомянуть о значимости третьего элемента предложенной Ю.Е. Максименко системы информационной безопасности – информационной безопасности в сфере прав и свобод человека и гражданина.

С учетом изложенного, рассмотренная выше концепция механизма обеспечения прав и свобод сельских жителей с помощью ИКИСМ может быть расширена в функциональном плане. В частности, она может быть дополнена такими категориями как объект информационной безопасности и субъект обеспечения информационной безопасности. При этом в роли объекта будет рассматриваться исключительно потребитель телекоммуникационных услуг, а в роли субъекта обеспечения будут выступать соответствующие субъекты властных полномочий и субъекты хозяйствования (например, операторы и провайдеры телекоммуникаций). Необходимо также учитывать, что концепция предлагаемого механизма ориентирована на активную форму участия сельских жителей в отношениях и процессах, связанных с созданием и функционированием ИКИСМ. Соответственно, рядовой житель сельской местности может и должен выступать также и в роли субъекта обеспечения собственной информационной безопасности. Однако практическая реализация этого теоретического вывода, прежде всего, нуждается в реализации мер образовательного и организационно-правового характера, нацеленных на преодоления таких явлений, как «информационный взрыв», «технологический шок» и «информационное неравенство».

**Выводы.** Завершая на этом работу, следует еще раз отметить, что в реалиях современной жизни «информационная эволюция» сельских территорий основывается именно на телекоммуникациях, и в этих условиях особую важность приобретает задача органи-

зационно-правового обеспечения информационной безопасности сельских жителей как потребителей телекоммуникационных услуг. В свою очередь, в процессе обеспечения этой безопасности нельзя пренебрегать одним из объектов кибернетической защиты государства – информационно-коммуникационной инфраструктурой сельской местности.

#### Список использованной литературы:

1. Волков Ю.В. Субъекты телекоммуникационного права: дис... канд. юрид. наук: спец. 12.00.14/ Ю.В. Волков. – Екатеринбург: Уральская государственная юридическая академия, 2008. – 195 с.

2. Сулацкий Д.В. Организационно-правовые засади забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг: дис... канд. юрид. наук: спец. 12.00.07 / Д.В. Сулацкий. – Херсон: Міжнародний бізнес та права, 2011. – 290 с.

3. План действий: Документ WSIS-03/GENEVA/DOC/5-R, (Женева, 12 декабря 2003 г.) [Электронный ресурс] / Веб-сайт ООН. – 14 с. – Режим доступа: <http://www.un.org/russian/conferen/wsis/plan.pdf>

4. Основы информационной безопасности: Учебное пособие для ВУЗов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

5. Сучасні тренди кібербезпекової політики: висновки для України: Аналітична записка [Електронний ресурс] / Д.В. Дубов; НІСД. – Режим доступу: <http://niss.gov.ua/articles/294/>

6. Недільніченко В.Д. Проблеми забезпечення безпеки об'єктів критичної інфраструктури з урахуванням впливу сучасних інформаційних технологій / В.Д. Недільніченко // Національна безпека: український вимір: зб. наук. зб./ РНБО України, Ін-т пробл. нац. безпеки; редкол.: В. П. Горбулін (голов. ред.) [та ін.]. – К.: ІПНБ РНБОУ, 2009. – № 6 (25). – С. 88-98.

7. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: автореф. дис... канд. юрид. наук: спец. 12.00.01 / Ю.Є. Максименко. – К.: КНУВС, 2007. – 22 с.

8. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис... доктора юрид. наук: спец. 12.00.07 / Б.А. Кормич. – Харків: НУВС, 2004. – 427 с.

9. Дотримання інформаційних прав і свобод українських громадян: нормативно-правове забезпечення і регулятивні важелі: Аналітичні записки щодо проблем і подій суспільного розвитку [Електронний ресурс] / С.Л. Гнатюк; НІСД. – Режим доступу: <http://www.niss.gov.ua/Monitor/May2010/01.htm>

10. Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України: проект Закону України, (реєстр. № 11125 від 31.08.2012) [Електронний ресурс] / Веб-сайт Верховної Ради України. – 7 с. – Режим доступу: [http://w1.c1.rada.gov.ua/pls/zweb\\_n/webproc34?id=&pf3511=44208&pf35401=231555](http://w1.c1.rada.gov.ua/pls/zweb_n/webproc34?id=&pf3511=44208&pf35401=231555)

11. Щодо розробки законопроекту про кібернетичну безпеку України: лист Державної служби спеціального зв'язку та захисту інформації на адресу Міністерства внутрішніх справ України. – 13.09.2012. – № 09/02/02-2981. – 9 с.

12. Про внесення змін до Закону України «Про основи національної безпеки України»: проект Закону України, (реєстр. № 2483 від 07.03.2013) [Електронний ресурс] / Веб-сайт Верховної Ради України. – 3 с. – Режим доступу: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=45998&pf35401=252706>

13. Модернізація України – наш стратегічний вибір: Щорічне послання Президента України до Верховної Ради України [Електронний ресурс] / Офіційне інтернет-представництво Президента України. – Режим доступу: [http://www.president.gov.ua/docs/Poslannya\\_sborka.pdf](http://www.president.gov.ua/docs/Poslannya_sborka.pdf)

14. Розвиток аграрного виробництва як передумова забезпечення продовольчої безпеки України/ О.В. Собкевич, В.М. Русан, А.Д. Юрченко, В.О. Скороход; за ред. Я.А. Жаліла. – Київ: НІСД, 2011. – 39 с.