Волжский университет имени В.Н. Татищева

ВЕСТНИК ПО БЕЗОПАСНОСТИ

№11 декабрь 2018

В НОМЕРЕ:

ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск одиннадцатый

Тольятти 2018

ББК 004.00+33.00+34.00+57.00+80/84

Материалы Всероссийской научно-практической конференции по безопасности. Вестник по безопасности. Выпуск одиннадцатый. – Тольятти: ВУиТ, 2018. - 105 с.

18-19 декабря 2018 года в Волжском университете имени В.Н. Татищева состоялась Всероссийская научно-практическая конференция по безопасности.

В настоящем издании публикуются материалы участников конференции.

Все материалы представлены в авторской редакции.

Ответственный редактор к. т. н., доцент О.Ю. Федосеева

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПРАВА СОБСТВЕННОСТИ ПО РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ

Ващенко Ю.С., к. ю. н., доцент
Волжский университет им. В.Н. Татищева
г. Тольятти

В данной статье проведен экономико-правовой анализ отношений собственности и его правовое регулирование по российскому законодательству.

Несмотря на достаточную проработанность института вещного права в трудах цивилистов, где базовым понятием является собственность, следует отметить, что законодательно он до сих пор не определён. Нет даже дефиниции этого понятия, так как всё традиционно сводится к триаде правомочий собственника — праву владения, пользования и распоряжения своим имуществом, за которыми и стоят названные законодательные определения данного понятия. Отчасти поэтому термин «собственность» употребляется в разнообразных значениях. Чаще всего его используют как синоним понятию «имущество» или «вещи», которые гражданским законом тоже не определены. Поэтому собственность — это определение скорее экономическое (фактическое отношение, подвергаемое правовому оформлению), которое состоит из отношения между людьми по поводу конкретных материальных благ (имущество, вещь), используемое собственником в своих интересах, так как к своему имуществу обычный человек относится иначе, чем к чужому. И последняя составляющая этого понятия, присвоение имущества (его передача, продажа и пр.).

Существует множество определений понятия собственности, с учётом своей специфики, у экономистов, которые своими направлениями, сложившимися школами разработали различные подходы и определения данной дефиниции. Выделим из них наиболее нейтральное – собственность - это отношение между субъектами рынка по поводу присвоения (отчуждения) средств производства и создаваемых с их помощью материальных благ в процессе производства, распределения, обмена и потребления.

У юристов собственность – это отношение собственника к несобственнику.

Что касается юридической составляющей, то право оформляет отношения между участниками экономического оборота по поводу имущества (моё — чужое), предоставляя его владельцу защиту от необоснованного посягательства иных лиц, а в отношении к присвоенному имуществу, определяет границы его дозволенного использования.

Следует отметить, что собственник вследствие своего хозяйственного господства над своим имуществом получает не только приятное «благо» его обладания, но и несёт бремя его содержания (должен заботиться, рисковать, включая потерю самого имущества), которое при утрате ему никто не компенсирует его стоимость, если оно не было им застраховано.

Не смотря на традиционно сложившееся восприятие «собственности» он всё же подвержен изменениям. Так в разделе II Гражданского кодекса РФ, регулирующего вещные права, полное его название звучит как «Право собственности и другие вещные права». Более того, входящие в него гл. 17 и 18 детализированы уже в самом оглавлении, их содержание наполнено конкретикой, помимо устоявшегося названия «права собственности» содержатся наименования «и другие вещные права на землю» (в ред. ФЗ от 16 апреля 2001 г. № 45-ФЗ), «и другие вещные права на жилые помещения». Это, безусловно, способствует развитию системы вещных прав, содержание правомочий которых закреплено в статье 216 ГК РФ (в ред. от 31.01.14 по состоянию на 15.10.18), где и установлен перечень вещных прав владеющего несобственника. Их список включает только общие правила относительно самих вещных прав. Эти вещные права владеющего пользователя конкретного имущества, которые порождают для данного субъекта целый комплекс правомочий.

Для того чтобы более полно раскрыть правовую природу правомочий собственности в

структуре основных понятий, рассмотрим сопутствующие этой триаде иные термины и терминообразования. Обратимся к истокам вещного права, которое пришло к нам из республиканского Рима, где названный институт осуществлял юридическую связь лица с вещью iura in re (право на вещь) и закреплял её за конкретным правообладателем. Принадлежность вещи презюмировалась самим законом, а характер защиты был подкреплён постулатом erga omnes в том смысле, что она адресована ко всем и будет действовать в случае его нарушения «против всех». В гражданском праве России, воспринявшем римскую традицию через пандектную систему гражданского права германской группы, вещные права именовались «неполными правами собственности» (ст. 432 т. X ч. 1 Свода законов Российской империи), содержались они и в ГК РСФСР 1922 г., используются и в действующем сейчас гражданском кодексе.

Отсюда вещные права — это одна из правовых форм реализации отношений собственности, которые предоставляют их обладателю возможность непосредственно (независимо от какого-либо другого лица) воздействия на вещь в своём интересе, с правом абсолютного господства. Само право собственности отличается от других вещных прав полнотой содержания, потому что никто из субъектов других вещных прав не имеет такой полноты правомочий на принадлежащее имущество. Объём их прав ограничен законом и собственником. Так, собственник, передавая часть своего имущества в оперативное управление или хозяйственное ведение другому лицу, сохраняет за собой право собственности на имущество.

Следует обратить внимание на то, что собственность в экономическом понимании (отношение лица к вещи) наиболее полно удалось проработать экономистам, которые выделили два ключевых термина - присвоение и отчуждение (у К. Маркса в «К критике Готской программы» эти термины упоминаются едва ли не впервые). Присвоение - это завладение чужой вещью, самовольный перевод в свою собственность; глагол «присвоить» означает доведение действия до конечной цели, которая содержит всю полноту исчерпанности самого действия; приблизиться к вещи (имуществу) настолько близко, что этот объект становится твоим. Антиподом присвоению является отчуждение, которое, в понимании того же С.И. Ожегова, означает «отбирать у кого-нибудь имущество в пользу государства, в частности, земельные участки, прилегающие к железной дороге», когда происходит прекращение и окончательное выполнение действия, связанное с переходом материальных объектов к новому собственнику.

Если приведённые примеры перевести на язык права, то отчуждение может происходить путём реквизиции на возмездных началах (ст. 242 ГК) или сопровождаться безвозмездной конфискацией имущества (ст. 243 ГК). Что касается смежных земельных участков, расположенных у железной дороги, то они в гражданском законодательстве легализованы в ст. 1331 ГК как линейные объекты, входящие в единый недвижимый комплекс и объединённые одним назначением. Естественно, что они составляют с железнодорожной линией одно целое.

Интересы экономических школ перекрещивались с правовыми оценками восприятия и понимания института собственности. Поэтому в самом римском праве для обозначения права собственности в экономическом смысле использовался термин «dominium», а в юридическом значении он воспринимался как «общее правовое господство лица над материальной вещью», которое обычно сопровождалось латинским постулатом «ex iure Quritium» (буквально «по праву квиритов», т. е. римских граждан).

В более поздний период в XX веке экономистами разных школ был разработан «пакет» прав, куда свою лепту внёс британский юрист А. Оноре («пучок прав Оноре»). Он разработал перечень прав, включающий в себя 11 элементов, значительно отличающийся от привычной триады правомочий собственника. Это: 1) право владения, т.е. исключительного физического контроля над вещью; 2) право пользования, т.е. личного использования вещи; 3) право управления, т.е. решения, как и кем вещь может быть использована; 4) право на доход, т. е. на блага, проистекающие от предшествующего личного пользования вещью или от разрешения другим лицам пользоваться ею (иными словами — право присвоения); 5) право

на «капитальную ценность» вещи, предполагающее право на отчуждение, потребление, изменение или уничтожение вещи; 6) право на безопасность, т.е. иммунитет от экспроприации; 7) право на передачу вещи по наследству или по завещанию; 8) бессрочность, нахождение вещи или имущества всецело зависит от желания (волеизъявления) самого собственника; 9) обязанность воздерживаться от использования вещи вредным для других способом; 10) ответственность в виде санкции, т.е. возможность отобрания вещи в уплату долга; 11) остаточный характер, т.е. ожидание «естественного» возврата переданных кому-либо правомочий по истечении срока передачи или в случае утраты ею силы по любой иной причине.

В рамках «пучка прав собственности» можно особо выделить два вида экономических прав: во-первых, права, связанные с извлечением полезных свойств объекта (его потребительной ценности) для определенных целей, – права хозяйственного ведения (скажем, – право пользования); во-вторых, права, связанные с возможностью передачи прав на управление другим контрагентам, – права собственности в узком смысле (например, – право распоряжения).

Поэтому собственность в представлении А. Оноре - это набор правомочий, которые в неодинаковых соотношениях и пропорциях распределяются между различными лицами. При этом не сами материальные блага с прочими ресурсами являются собственностью, а «обмен пучками прав собственности», где, по мысли того же А. Оноре, при ограниченности ресурсов на земле и доступа к ним бессмысленно вести разговор о собственности как таковой. Собственником может стать каждый, но если исходить из экономической теории прав собственности, то не сам ресурс является собственностью, а «пучок прав». Особенно если они к тебе переходят во временное владение и пользование (скажем, на праве аренды), то здесь следует говорить уже о некой конструкции, как временная собственность, которая полной и постоянной, тем более своей, никогда не станет, если аренду, конечно, не оформить с правом последующего выкупа арендуемого объекта. Отсюда, с точки зрения экономистов, триада правомочий - это далеко не полная собственность. К примеру, никакое государство никогда не передаст в собственность тот же шельф или свои недра другому государству, за исключением тех ресурсов, которые ничьи, и на них не существует никаких ограничений в плане доступа к использованию. Правда, назвать это собственностью нельзя, потому что собственность только тогда имеет свою реальную стоимость, если она включена в гражданский оборот (путём купли-продажи, поставки, аренды и пр.).

Продолжая разговор о собственности, перейдём к триаде правомочий собственности с характерным содержанием каждого из этих прав и его особенностями. Традиционно на первом месте, из имеющихся правомочий всегда стоит владение (ius possidendi), очень ёмкое понятие с большой семантической глубиной, которое при известных условиях могло рассматриваться как обеспеченное законом фактическое обладание вещью. Основанием владения может быть не только «право самого собственника, но и право другого собственника, включая отсутствие всякого права владеющего несобственника». Само право, имеющее римские корни, возникало по иным основаниям, например если человек приобрёл вещь у того лица, которое не могло продавать эту вещь, или она была краденой. Это объясняется тем, что в древнеримском праве различали просто владение (possession) и фактическое обладание, т.е. «телесное» владение (corpus possidendi). Отсюда владение в Риме это не только фактическое обладание, но и желание воспользоваться вещью как своей. В известных случаях владение могло перерасти в собственность. Скажем, человек, получивший на временное хранение вещь, по факту обладающий ею (спрятал или закрыл на замок), не являлся её владельцем, а только был фактическим обладателем, держателем вещи (detentor). Но если фактический обладатель вещи решался её как-то использовать для себя (вещь при мне, она у меня «прижилась»), он превращался во владельца, причём незаконного, поэтому и считалось, что он совершил кражу.

Но у юристов есть (были) и другие точки зрения. Так, Р. Иеринг считал, что в римском праве владение приравнивалось к фактическому обладанию. Однако римский юрист Ульпиан

противопоставлял владение и собственность, говоря, что собственность не имеет ничего общего с владением (Дигесты, 41.2.12). У римского юриста были свои основания считать так, которые и привели его к этому выводу. Но эти рассуждения выходят за рамки нашей статьи.

Право собственности определялось как право пользования с правом приобретения и потребления тех же плодов, включая и право распоряжения. С принадлежностью вещи конкретному лицу (владеть можно только вещью, исходя из специфики объекта вещных прав). В нём также находило своё выражение состояние «присвоенности», физического обладания и власти над вещью. Что служит лишним доказательством сказанного Р. Иерингом: «Где нет собственности, там нет владения».

Ошибочным было бы считать, что владение порождает для субъекта фактическое господство над вещью, так как, невзирая на то, что данное право исключает притязания на саму вещь всех третьих лиц, тем не менее, наш законодатель сознательно сам допускает притязания, исключить влияние которых полностью нельзя. Например, присутствующие в юридических текстах при сделках с юридическими лицами дефиниции «слияние» и «поглощение» (дружественное или недружественное) рассматриваются с применением института корпоративного договора, конструкции заверений об обстоятельствах, других устанавливающих право документов, на основании которых и создаётся правовая основа, порой оправдывающая отъём собственности у её законных владельцев. В судебной практике последних лет достаточно подобных примеров. Тем более, что арбитражные суды по однородным делам выносят противоположные решения, хотя по данной категории дел есть соответствующее решение Конституционного Суда РФ.

Одно из самых распространённых в литературе определений данного правомочия владения всегда идёт в согласовании со словосочетанием «господство над вещью». Здесь следует привести точку зрения проф. Д.М. Генкина, что «понятие господства лица над вещью является нежелательным для правовой теории, рассматривающей отношения между людьми, а не отношения между людьми и вещами», так как в некоторых случаях «бывает трудно определить, существует ли в конкретном случае владение или нет».

Тем не менее, следует отметить, что термин «господство (господствовать) над вещью» (см. п. 1.2 подразд. 1 «Владения» разд. IV «Законодательство о вещных правах»), получил свою прописку не только в гражданском законодательстве, но и в земельном кодексе тоже.

К написанному следует сказать, что «юридический владелец без освоения владения «пустой господин» leerer Herr, а настоящий собственник по праву свободы собственности тот, кто делает из неё употребление».

Здесь мы переходим ко второй составляющей правомочия собственности - «пользование», которое в литературе рассматривается как фактическое использование имущества путём извлечения из него полезных свойств (ius utendi et ius fruendi). Его связь с владением более чем наглядна, так как пользоваться можно только тем имуществом, которым ты владеешь. Более того, неиспользование имущества или его нецелевое использование может стать основанием прекращения данного права пользования (см. ст. 240, 241, 260, 284-286, 293 ГК РФ).

Если обратиться к смысловой основе слова «пользования», это только подтверждает, что мы говорили, когда сравнивали его с «владением». Здесь не только «извлечение выгоды для себя из чего-нибудь, но и обладание чем-нибудь; иметь что-то». Владимир Даль, анализируя это значение, считал, что оно произошло от слова «польза» и близкого к нему «польга». Если первое означает «выгода, прибыль, барышъ», то второе имело смысл «льгота, облегчение». Отсюда в пользовании синтезировались два смысла: извлекающий прибыль и приносящий пользу при использовании.

Близким, тесно связанным с пользованием является правомочие «распоряжение» (ius dispo-nendi), которое предполагает совершение с вещами (имуществом) различных юридически значимых действий, тех же сделок, совершение которых позволит изменить «юридическую судьбу» вещи путём отчуждения, отказа, передачи, вплоть до уничтожения. В связи с чем меняется правообладатель-собственник (или иной пользователь), по желанию которого устанавливается правовой режим вещи и в итоге определяется её правовая принадлежность.

Семантико-грамматическая сторона термина «распоряжение» осложнена дихотомией его понимания. Практически все словарные источники сводят эту дефиницию к функции управления, принятию решения, с последующей отдачей приказа по определению судьбы имущества, заботясь об устройстве, использовании и применении его другим лицом в дальнейшем. Здесь властно-распорядительная модель подкрепляется правоустанавливающими документами. Так, в административном и конституционном праве это акт управления, имеющий властный и волевой характер. Издают его либо управомоченный на его издание орган, государственный либо какой-нибудь иной орган или субъект (должностное лицо) управленческой деятельности в пределах своей компетенции. В гражданском праве собственник вещи или имущества, а также субъекты прав оперативного управления или хозяйственного ведения, имея возможность реализовать имущество, включают его в гражданский оборот (путём купли-продажи, дарения, поставки и др.). Распоряжаясь вещью путём отчуждения, они определяют её юридическую судьбу.

Теперь что касается этимологии, то «распоряжение» ведёт своё начало от глагола «распоряжать (распорядить)», что при всей многозначности его прочтения понимается как «править, управлять, принимать меры, отдавать приказанья», а вот производное от них слово «распорядничать» воспринимается как «распоряжаться и хозяйничать, заводить порядок». Само слово «порядокъ» многозначное, применительно к нашему случаю оно включает в себя «торговый ряд, уговоръ, условье и сделку».

В первом случае это соотносится с административно-конституционным началом, а во втором вполне укладывается в гражданско-распорядительную модель отношений.

Данное правомочие очень замкнуто на юридическом значении собственности, так как определить юридическую судьбу имущества без установленной процедуры (самого порядка), которая определяется нормами Федерального закона от 21.07.1997 № 122-ФЗ (в ред. от 13.07.2017) «О государственной регистрации прав на недвижимое имущество и сделок с ним», без соответствующей регистрации права собственности на конкретное имущество не представляется возможным.

Поэтому под правом собственности понимаются как санкционированные обществом (законами государства, традициями, обычаями, распоряжениями администрации и т.д.) общественные (поведенческие) отношения между людьми, которые возникают в связи с существованием различных как материальных, так и нематериальных благ в процессе их производства, распределения, обмена и потребления.

В содержании собственности лежит понятие "присвоение", которое включает в себя – владение, пользование и распоряжение.

В заключение статьи следует признать, что подходы и взгляды на имеющиеся правомочия собственности как с юридической, так и экономической стороны, достаточно устоявшиеся и традиционные. Тем не менее следует отметить, что экономические школы с их различными подходами и определениями самого понятия собственности рассматривают данный институт в отличии от тех же юристов со своими экономическими особенностями, так как, именно, собственность является основным и системообразующим видом экономических отношений, которая формирует все остальные виды.

Библиографический список

1. Onore, A. Ownership // Oxford Essays in Jurisprudence / ed. by A.W. Guest. Oxford, 1961. P. 112-128.

2. Бибихин, В.В. Собственность. Философия своего. СПб.: Наука, 2012.

3. Грешников, И.П. Субъекты гражданского права: юридическое лицо в праве и законодательстве. СПб.: Юрид. центр Пресс, 2002. С. 7.

4. Даль, В. Толковый словарь живого великорусского языка. М.: Русский язык, 1981.

5. Иеринг, Р. Об основании защиты владения. М., 1992. С. 116.

6. Кружалова, Л.В. Римское частное право. 2-е изд. СПб., 2009. С. 124.

7. Кузнецова, Л.В. Вещные права на имущество и бремя его содержания // Вещные

права: постановка проблемы и её решение: сб. статей. М.: Статут, 2011. С. 14.

8. Латыев, А.Н. О владении по Концепции развития гражданского законодательства // Вещные права: постановка проблемы и её решение: сб. статей. М.: Статут, 2011. С. 64-66.

9. Маркс, К.К критике политической экономии. М.: Мысль, 1962.

10. Обращение акций в акционерном обществе [Электронный ресурс] – Режим доступа: URL: BiznesLuxe.ru.

11. Ожегов, С.И. Словарь русского языка. М.: Русский язык, 1981. С. 494.

12. Победоносцев, К.П. Курс гражданского права. М., 2002. С. 586.

13. Потиха, З.А. Строение русского слова. М.: Русский язык, 1981. С. 286-287.

14. Скловский, К.И. Собственность в гражданском праве. М.: Статут, 1999. С. 167.

15. Словарь русского языка XI-XVII вв. Вып. 2 (В - Волога). М.: Наука, 1975. С. 209.

16. Тархов, В.А., Рыбаков, В.А. Собственность и право собственности. Уфа: Изд. Уфимского юридического института МВД РФ, 2000. С. 103.

17. Черных, П.Я. Историко-этимологический словарь современного русского языка. 8-е изд. М., 2007. Т. 1. С. 156-157.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДОГОВОРА РЕНТЫ В РОССИИ

Воровко К.Я., Ганюшова Е.Ю., студенты
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет им. В.Н. Татищева
г. Тольятти

Договор ренты один из распространенных договоров российского гражданского оборота. Несмотря на это он является достаточно новым видом договора для современного законодательства. Как известно данный институт в науке был известен давно, однако на законодательном уровне он был закреплен лишь в Гражданском кодексе Российской Федерации 1996 года.

При этом предпосылки к формированию этого института наблюдаются уже в Гражданском кодексе РСФСР 1964 года, несмотря на то, что глава, посвященная ренте, в нем отсутствовала, он содержал несколько статей посвященных купле-продаже жилого дома с условием пожизненного содержания продавца. Такие отношения предусматривались в тех случаях, когда жилые дома отчуждались нетрудоспособными гражданами, другим лицам, бравшим на себя обязательство по пожизненному содержанию данного нетрудоспособного лица[1]. Данная норма схожа с положением о пожизненном содержании с иждивением, закрепленным в настоящем кодексе. Из этого следует, что договор ренты начинает свое формирование с этого вида.

Окончательно институт ренты был сформирован после принятия в 1996 году Гражданского кодекса Российской Федерации (далее ГК РФ). Именно с этого момента законодатель четко сформировал положения договора ренты, указал стороны договора, определил их права и обязанности, а также условия необходимые для осуществления данного договора. В отличие от других договоров в новом ГК рентные отношения урегулированы практически исчерпывающим образом и не содержат, за редким исключением, отсылок к иным актам законодательства. Глава 33 настоящего кодекса «Рента и пожизненное содержание с иждивением» содержит как общие нормы о ренте, так и специальные. Полное определение договора ренты закреплено в п. 1 ст. 583 ГК РФ. В ней указано, что по договору ренты одна сторона (получатель ренты) передает другой стороне (плательщику ренты) в собственность имущество, а плательщик ренты обязуется в обмен на полученное имущество периодически выплачивать получателю ренту в виде определенной денежной суммы либо предоставление

[1] Гражданский кодекс РСФСР «Гражданский кодекс РСФСР» от 11.06.1964 // Российская газета.

средств на его содержание в иной форме[1].

Несмотря на то, что рента как гражданско-правовой институт – это новелла в законодательстве, в литературе уже имеются различные точки зрения по ряду вопросов, касающихся его положений. Разногласия начинаются с вопроса о количестве видов договора ренты, а точнее: является ли договор пожизненного содержания с иждивением видом или подвидом договора ренты. Высказываются совершенно противоположные точки зрения: одни выделяют три договора ренты (постоянная, пожизненная и пожизненное содержание с иждивением); другие относят пожизненное содержание с иждивением к виду пожизненной ренты, то есть подвиду ренты, различая как виды пожизненную и постоянную ренту. В силу того, что данный договор нашел свое нормативно-правовое регулирование в гражданском законодательстве, закреплен в ст. 601 ГК РФ, а также сложившейся судебной практики и по мнению цивилистов, которые определяют его как отдельный вид договора ренты, мы согласны с первой точкой зрения.

Так же в литературе существует точка зрения, что договор ренты – это «односторонний договор». Хотя известно, что договор ренты по своей природе является двусторонним, возмездным, реальным. Такая позиция представляется неточной хотя бы в силу статьи 154 ГК РФ, проводящей разграничение односторонних сделок, для совершения которых в соответствии с законом, иными правовыми актами или соглашениями сторон необходимо и достаточно выражение воли одной стороны, и договоров, для заключения которых необходимо выражение согласованной воли двух сторон (двусторонняя сделка) либо трех или более сторон (многосторонняя сделка)[2].

В данной статье речь пойдет о договоре пожизненного содержания с иждивением. Сущность данного вида договора отражена в статье 601 ГК РФ, так в п. 1 данной статьи указано: «по договору пожизненного содержания с иждивением, получатель ренты – гражданин передает принадлежащие ему жилой дом, квартиру, земельный участок или иную недвижимость в собственность плательщика ренты, который обязуется осуществлять пожизненное содержание с иждивением гражданином и (или) указанного им третьего лица (лиц)»[3]. Мы видим, что специфической чертой данного вида договора является переход в собственность плательщика только недвижимого имущества, что и отличает его от договоров постоянной и пожизненной ренты. Законодатель к тому же определил перечень объектов свойственных этому договору.

Сторонами данного договора являются получатель ренты и плательщик ренты, между которыми существует достаточно тесная взаимосвязь, что также отличает договор пожизненного содержания с иждивением от других видов ренты, в которых отношения сторон ограничиваются передачей (перечислением) денежных средств или иного оговоренного договором предоставления при отсутствии, как правило, личных контактов. Говоря о тесной взаимосвязи сторон данного вида договора, имеется в виду то, что получатель ренты, возлагая на плательщика обязанности по обеспечению потребности в жилище, питании, одежде и т.п., доверяет ему и находится с ним в психологическом взаимодействии.

Статья 604 ГК РФ содержит положения о том, что плательщик ренты способен осуществлять определенные действия (отчуждать, сдавать в залог или иным способом обременять недвижимое имущество) в отношении объекта, полученного в собственность по этому договору только с предварительного согласия получателя ренты[4]. Содержание этой нормы позволяет квалифицировать договор пожизненного содержания с иждивением как договор доверительного (фидуциарного) характера.

---

[1] Закон Российской Федерации "Гражданский кодекс Российской Федерации " от 30 ноября 1994 № 51-ФЗ // Российская газета.

[2] Гражданское право. Особенная часть в 2 Т. Том 1 / Анисимов А.П., Козлова М.Ю., Рыженков А.Я., Чаркин С.А., под ред. Рыженкова А.Я. - 6-е изд. - М.: "Юрайт", 2018. - С. 79.

[3] Закон Российской Федерации "Гражданский кодекс Российской Федерации" от 30 ноября 1994 № 51-ФЗ // Российская газета.

[4] Там же.

При заключении договора стороны конкретизируют условия, качество, форму каждого вида предоставления, однако стороны могут пойти дальше и зафиксировать в договоре их величину в стоимостном выражении. Законодатель в п. 2 ст. 602 ГК РФ указывает общую стоимость всего объема содержания с иждивением, размер которого не может быть менее двух минимальных размеров оплаты труда, установленных законом[1].

Исходя из того, что стороны проживают на совместной территории, в силу специфики договора, заключенного ими, они вынуждены детально оговаривать порядок своего взаимодействия. Так закон дает им право самостоятельно определить периодичность предоставления содержания, отталкиваясь от необходимости обеспечения нормальных естественных потребностей человека.

Изучив договор ренты, а конкретнее, пожизненное содержания с иждивением, можно указать на права и обязанности сторон. Так получатель ренты обладает достаточно широким кругом прав. Он может на законных основаниях рассчитывать на получение рентной платы в виде содержания с иждивением, другими словами, получатель на протяжении жизни имеет право на обеспечение своих нужд в жилище, еде, уходе, одежде, а также покрытии расходов на ритуальные услуги. Ему могут предоставляться иные блага, предусмотренные в договоре. В обязанности получателя ренты входит обязанность по передачи принадлежащего ему имущества (обязательно недвижимого) в собственность плательщика, в случае выполнения им своих обязательств.

Плательщик ренты в свою очередь обладает следующими правами: в соответствии с договором, он имеет право принять в собственность принадлежащее получателю недвижимое имущество, также закон предоставляет ему возможность отчуждать (продавать, дарить, сдавать в залог) принятое имущество, но при этом как уже упоминалось, законодатель вводит поправку и указывает в ст. 604 ГК РФ, что делать это можно лишь с согласия получателя ренты. Главной обязанностью плательщика ренты выступает обязанность выполнять свои обязательства по уплате ренты в виде содержания с иждивением рентополучателя[2].

Очевидным становиться, что получатель и плательщик ренты не равны, при реализации предоставленных им прав и обязанностей. В данном случае круг прав получателя ренты достаточно широкий, чего нельзя сказать о правах плательщика ренты, даже его право на отчуждение полученного имущества ограничивается законодателем, который указывает, что плательщик не всегда и не в любой момент может осуществить предоставленное ему право, а лишь тогда, когда на это даст добро получатель ренты.

Таким образом, уязвимой стороной данного договора, на наш взгляд, является именно плательщик ренты, хотя закон стоит именно на стороне получателя. Конечно, на первый взгляд это может показаться верным, в связи тем, что получатель считается стороной, нуждающейся в более эффективной правовой защите, и им может стать лишь такое лицо, которое в силу состояния здоровья или иных обстоятельств нуждается в пожизненном содержании до конца жизни. К тому же на практике встречается немало примеров, когда, заключая договор пожизненного содержания с иждивением, пожилые люди подвергаются серьезному риску, заключая договор не с добропорядочными плательщиками, а с мошенниками.

В чем же заключается уязвимость плательщика ренты? Дело в том, что данный договор при всей своей привлекательности содержит значительную долю риска, сопряженную с личностным характером сделки и возможными противоречиями между сторонами, возникающими, как правило, уже в процессе реализации договора. Как уже было сказано, обязанности получателя ренты ограничиваются лишь передачей его имущества плательщику, а обязанности плательщика ренты содержат более широкий перечень, в это случае проблема состоит в том, что сложно соотнести гражданско-правовые положения договора с возможным возникновением и последствиями конфликтов не правового, а личного характера в процессе предоставления пожизненного содержания с иждивением, построенного именно на тесном личном

[1] Закон Российской Федерации "Гражданский кодекс Российской Федерации " от 30 ноября 1994 № 51-ФЗ // Российская газета.

[2] Иванова Е.В Договорное право в 2 Т. Том 2. Особенная часть. - 2-е изд. - М.: Гриф УМО ВО, 2018. - С. 63.

контакте плательщика и получателя ренты.

Есть и еще один нюанс, позволяющий признать плательщика ренты уязвимой стороной. Ни для кого не секрет, что данный договор заключается на срок, который ограничивается смертью получателя ренты, в таком случае плательщик ренты, заключающий такое соглашение может лишь предполагать, на какой период продляться его обязательства в пользу получателя ренты. Предположим, к примеру, что смерть получателя ренты наступила по истечении трех лет с момента заключения договора, а если получатель ренты окажется завидным долгожителем, который, к примеру, доживет до внушительного возраста, при этом сейчас ему шестьдесят. В подобном случае, может возникнуть ситуация, что и сам плательщик может не дожить до того момента, когда он сможет самостоятельно, без согласия получателя, распоряжаться правом собственности на переданное ему имущество.

Что касается расторжения договора пожизненного содержания ренты, то следует учитывать, что данный договор в силу своей природы прекращается со смертью получателя ренты, о чем говорилось ранее[1]. Однако, предусмотрена процедура отказа от договора, в случае если одна из сторон передумала. Важным является то, что подобные действия возможны лишь по обоюдному согласию сторон, что и делает эту процедуру довольно сложной. Также для этого должны быть веские причины, например, такие как:

— длительная задержка или полное отсутствие рентных выплат;

— задержка по оплате коммунальных платежей, но только в том случае, если такая обязанность возложена на плательщика ренты;

— иные веские причины, которые нарушают договорные отношения сторон;

При наличии подобных причин, отказ договора производится двумя способами, он может быть осуществлен путем заключения соглашения о расторжении договора пожизненного содержания с иждивением, заверенного нотариусом или путем судебного разбирательства, в котором принимают участие стороны этого договора.

Стоит также уточнить, что случайная гибель или случайное повреждение имущества, переданного под выплату пожизненной ренты, ответственность, за сохранность которого возложена на плательщика, не является основанием для прекращения рентных обязательств и основанием для расторжения договора пожизненного содержания с иждивением[2].

Практика показывает, что первопричиной требований получателя ренты о расторжении договора часто является не нарушение плательщиком ренты своих обязательств, а именно конфликты и разрыв в личных взаимоотношениях, на которых впоследствии строятся взаимные обвинения сторон. В том числе материального характера[3].

При детальном анализе договора пожизненного содержания с иждивением, мы делаем вывод, что данный договор является отдельным видом договора ренты наравне с постоянной и пожизненной рентой, а не подвидом. Он достаточно четко регламентирован законодателем, однако на наш взгляд необходимо более обширно урегулировать права плательщика ренты, в связи с тем, что риск прекращения рентных взаимоотношений для него наиболее высок, нежели чем для получателя. Связанно это с тем, что данный договор тесно связан с личными взаимоотношениями сторон, в результате чего не один плательщик ренты просто-напросто не застрахован от «наговора», т.е. обвинения его в ненадлежащем исполнении своих обязательств, при этом, бремя доказывания по добросовестному выполнению своих обязанностей лежит на самом плательщике.

[1] Зенин И.А. Гражданское право. Особенная часть. - 18-е изд. - М.: "Юрайт", 2018. - С. 80.

[2] Гражданское право. Особенная часть в 2 Т. Том 1 / Анисимов А.П., Козлова М.Ю., Рыженков А.Я., Чаркин С.А., под ред. Рыженкова А.Я. - 6-е изд. - М.: "Юрайт", 2018. - С. 84.

[3] Зенин И.А. Гражданское право. Особенная часть. - 18-е изд. - М.: "Юрайт", 2018. - С. 79.

ПОНЯТИЕ И ПРИЗНАКИ БАНКРОТСТВА ГРАЖДАНИНА В ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Гаврилов И.А., студент
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет им. В.Н. Татищева
г. Тольятти

В правовой системе Российской Федерации сложилась исключительная ситуация, в соответствии с которой нормы о несостоятельности физического лица (гражданина) присутствуют в федеральном законодательстве на протяжении уже более восемнадцати лет, однако до 1 октября 2015 года указанные нормы фактически не применялись.

Первой попыткой введения механизмов банкротства граждан в Российской Федерации стало вступление в силу Федерального закона «О несостоятельности (банкротстве)» от 08.01.1998 г. № 6-ФЗ. Согласно п. 2 ст. 185 данного Закона положения о банкротстве граждан должны были вступить в законную силу с момента принятия Федерального закона о внесении соответствующих изменений в Гражданский кодекс Российской Федерации (далее – ГК РФ), который впоследствии так и не был принят[1].

Действенный механизм взыскания долгов с гражданина в российском законодательстве по-прежнему отсутствовал. Попытки разрешения конфликта между гражданином и его денежными кредиторами не были сконцентрированы на механизмах помощи гражданину-должнику, попавшему в сложную финансовую ситуацию, а были перенесены либо в сферу исполнительного производства, либо переводились во внеправовую сферу разрешения денежных конфликтов, зачастую носящую криминальный и полукриминальный характер[2].

Второй попыткой введения механизмов банкротства граждан явилось принятие Федерального закона «О несостоятельности (банкротстве)»[3] от 26.10.2002 г. № 127-ФЗ (далее – ФЗ «О несостоятельности (банкротстве)»). В главе X названного выше Закона содержались нормы о банкротстве гражданина. Однако на практике механизмы банкротства граждан так и не были применены[4] в силу п. 2 ст. 231 ФЗ «О несостоятельности (банкротстве)».

Наступивший осенью 2008 года финансовый кризис обнажил острую потребность в социально ориентированном правовом инструменте по регулированию положения гражданина-должника.[5]

В период с 2010 по 2013 год общий объем кредитов, выданных гражданам, вырос с 4 трлн рублей почти до 9 трлн рублей. Аналитики большинства кредитных организаций стали отмечать, что бремя кредитного долга населения превысило все допустимые рамки. Согласно данным аналитиков АО «Альфа-банк», долг по кредитам каждого пятого заемщика в России превышает реальную возможность его погашения из заработной платы[6].

Ввиду сложившихся обстоятельств, в конце 2014 года законодатель предпринял третью попытку введения механизмов банкротства граждан путем принятия Федерального закона «О внесении изменений в Федеральный закон О несостоятельности (банкротстве) и отдельные законодательные акты Российской Федерации в части регулирования реабилитационных

---

[1] Собрание законодательства Российской Федерации. 1998. № 2. Ст. 222.

[2] Фролов И.В. Банкротство гражданина: проблемы введения и модели правового регулирования. // Законы России: опыт, анализ, практика. 2016, №2. С.96.

[3] Собрание законодательства Российской Федерации. 2002. № 43. Ст. 4190.

[4] Постановление Пленума Высшего Арбитражного Суда РФ № 29 «О некоторых вопросах практики применения Федерального закона «О несостоятельности (банкротстве)» от 15 декабря 2004 г. (в ред. от 21 декабря 2017 г. Постановление Пленума ВС РФ № 53). Доступ из справ.-правовой системы «Консультант Плюс».

[5] Железняк А. Банкротство гражданина. Истинные цели и первый опыт правоприменения. // ЭЖ-Юрист. 2016, №22. С. 5.

[6] Докучаев Д.С. Дефолт на душу населения. // Новая газета. 2013, №88. С. 11.

процедур, применяемых в отношении гражданина-должника» от 29.12.2014 № 476-ФЗ[1]. В новой редакции была принята статья 25 ГК РФ. Она стала называться «Несостоятельность (банкротство) гражданина». Были внесены изменения в главу X «Банкротство гражданина» ФЗ «О несостоятельности (банкротстве)», закрепляющие институт банкротства граждан-потребителей. В Гражданский процессуальный кодекс Российской Федерации (далее – ГПК РФ) была внесена глава 32.1 «Признание гражданина несостоятельным (банкротом)». Законодатель относил рассмотрение дел о несостоятельности (банкротстве) граждан-потребителей к подведомственности судов общей юрисдикции. Указанный закон должен был вступить в силу с 1 июля 2015 года.

Крайней неожиданностью для юридического сообщества стало принятие Федерального закона «Об урегулировании особенностей несостоятельности (банкротства) на территориях Республики Крым и города федерального значения Севастополя и о внесении изменений в отдельные законодательные акты Российской Федерации» от 29 июня 2015 г. № 154-ФЗ[2]. Данный закон регламентировал новую редакцию статьи 25 ГК РФ, в частности, закрепив положение о признании гражданина банкротом по решению арбитражного суда. Так же названным выше законом отменена редакция параграфа 1.1 главы X ФЗ «О несостоятельности (банкротстве)», принятая в декабре 2014 года, и принята новая редакция данного параграфа[3]. Это явилось четвертой и финальной попыткой законодателя по введению механизмов банкротства граждан в Российской Федерации.

На сегодняшний день институт банкротства – определенная организация общественной деятельности и социальных отношений, которая воплощает в себе нормы экономической, политической, правовой, нравственной жизни общества, а также социальные правила жизнедеятельности и поведения людей[4]. Банкротство граждан невозможно называть классической гражданско-правовой конструкцией, основанной на свободе воли и диспозитивных началах. Оно имеет ряд существенных отличий от института банкротства юридических лиц, ключевыми целями которого являются пропорциональное удовлетворение требований кредиторов и освобождение рынка от субъектов, неспособных осуществлять рациональное хозяйствование. В банкротстве граждан преобладает публичный элемент ввиду идеи социальной реабилитации. Главной задачей является восстановление активности должника в социальной и экономической жизни[5]. Именно это положение существенно влияет на природу нормативного регулирования механизма банкротства граждан.

При таких обстоятельствах несостоятельность (банкротство) гражданина как правовой инструмент позволяет добросовестным, экономически активным гражданам, попавшим в трудную финансовую ситуацию, оставаться вовлеченными в экономические процессы.

Институт несостоятельности (банкротства) граждан включает в себя четыре самостоятельных элемента: банкротство физического лица (гражданина), банкротство индивидуального предпринимателя, банкротство крестьянского (фермерского) хозяйства и банкротство гражданина в случае его смерти, которые имеют ряд существенных различий в своей правовой природе[6].

Легальное понятие несостоятельности дано в статье 2 ФЗ «О несостоятельности (банкротстве). Несостоятельность (банкротство) - признанная арбитражным судом неспособность должника в полном объеме удовлетворить требования кредиторов по денежным обязательствам, о выплате выходных пособий и (или) об оплате труда лиц, работающих или работав-

[1] Собрание законодательства Российской Федерации. 2015. № 1. (часть I). Ст. 29.

[2] Собрание законодательства Российской Федерации. 2015. № 27. Ст. 3945.

[3] Алексеев А.А. Проблемы и особенности введения института несостоятельности (банкротства) физических лиц в России. // Имущественные отношения в РФ. 2016, №4. С. 79.

[4] Новоселова А.Н. Правовая природа института банкротства физических лиц в России. // Academy. 2018, №2(29). С. 57.

[5] Свириденко О.М. Принцип объективной реальной платежеспособности должника // Актуальные проблемы российского права. 2016, № 11. С. 100.

[6] Карелина С.А. Институт банкротства граждан по законодательству РФ. // Предпринимательское право. Приложение «Право и Бизнес». 2017, №4. С. 8.

ших по трудовому договору, и (или) исполнить обязанность по уплате обязательных платежей.

В силу прямого указания п. 1 ст. 213.1 Закона о несостоятельности отношения, связанные с банкротством граждан и не урегулированные главой X, регулируются главами I - III.1, VII, VIII, параграфом 7 главы IX и параграфом 2 главы XI ФЗ «О несостоятельности (банкротстве)». Данное положение означает, что признаки банкротства гражданина определяются по тем же правилам ст. 3 ФЗ «О несостоятельности (банкротстве)», что и признаки банкротства юридического лица[1].

Следовательно, гражданин считается неспособным удовлетворить требования кредиторов по денежным обязательствам, о выплате выходных пособий и (или) об оплате труда лиц, работающих или работавших по трудовому договору, и (или) исполнить обязанность по уплате обязательных платежей, если соответствующие обязательства и (или) обязанность не исполнены им в течение трех месяцев с даты, когда они должны были быть исполнены.

На текущий момент при определении признаков банкротства гражданина используется критерий неплатежеспособности. Законодательное определение неплатежеспособности приводится в статье 2 ФЗ «О несостоятельности (банкротстве)»: это прекращение исполнения должником части денежных обязательств или обязанностей по уплате обязательных платежей, вызванное недостаточностью денежных средств[2].

Дела о банкротстве граждан рассматриваются арбитражными судами по месту жительства граждан-должников. Согласно статье 3 Федерального конституционного закона от 28.04.1995 № 1-ФКЗ «Об арбитражных судах в Российской Федерации», в качестве арбитражных судов первой инстанции выступают суды субъектов Российской Федерации, которые находятся в центральных регионах[3]. В заявлении необходимо указать саморегулируемую организацию арбитражных управляющих, из состава которой будет утверждаться финансовый управляющий.

Отметим, что правовая система России совсем недавно приобрела концептуально новый институт потребительского банкротства. Банкротство граждан имеет ряд существенных отличий от несостоятельности юридических лиц, что проявляется в содержании и целях названного института. Личность гражданина-должника, его права и свободы имеют первостепенное значение. Ключевой целью процедуры банкротства гражданина является создание правовых условий, которые, в свою очередь, поспособствуют реабилитации участника гражданского оборота.

ИСТОРИЯ ВОЗНИКНОВЕНИЯ ИНСТИТУТА НЕСОСТОЯТЕЛЬНОСТИ

Девадзе С.Г., студент
Научный руководитель: Галеева Г.Р., к. ю. н.
Волжский университет им. В.Н. Татищева
г. Тольятти

Правовое регулирование банкротства впервые появляется в римском праве. С момента возникновения частной собственности, действующие законы и правила не были милосердны к должникам. Изначально, в качестве гарантии обеспечения возврата долга, предусматривались не столько имущественные, сколько личные последствия несостоятельности должника. И выражалось это в том, что кредитор был вправе убить должника. Так, в Римском праве еще в 12 столетии было записано, что кредиторы, не получившие удовлетворение своих претензий, имеют право разрубить своего должника на части.

[1] Белых В.С. Банкротство граждан (Критерии. Статус. Процедуры): учебно-практическое пособие. / под общ. ред. В.С. Белых. М.: Проспект, 2016. С. 34.

[2] Суровцева Н.А., Белопашенцева К.В. Российское законодательство о банкротстве. // Молодой ученый. 2018, №19. С. 79.

[3] Собрание законодательства Российской Федерации. 1995. № 18. Ст. 1589.

В период с IX- X веков Италия развивалась, как торговая страна. И именно торговцы чаще всего оказывались неплатежеспособными. За счет чего и появляется необходимость в регулировании так называемой «торговой неплатежеспособности». Появлению на свет понятия «банкрот» современное право обязано итальянскому. Так в XIII века в Италии будет сформирован термин «банкротство» - от bancarotta (bancus - «лавка, торговое заведение» и rotto - «ломать, закрывать заведение») - «закрытая лавка», «перевернутый стол менялы», что под собой понимало полный крах торговца, и, как правило, его скорый побег от кредиторов. Объявление банкротом и контроль за осуществлением необходимых после этого к банкроту мер осуществлял суд, но при весомом участии кредиторов.

Стоит отметить, что также не мало важным этапом, как и появление термина «банкротство», в истории развития конкурсного права стало Торговое уложение, принятое 12 сентября 1807 года и вступившее в силу с 1 января 1808 года во Франции. Оно касалось исключительно вопросов торговой несостоятельности. В нем устанавливалось, что только купцы могут быть признаны несостоятельными. Лица же, не ведущие торговлю, могут впадать в неоплатность, которая впоследствии влечет иные последствия и рассматривается общими судами. Уложение усилило уголовную направленность норм и закрепило три вида несостоятельности: несчастную, неосторожную и злостную. Любой должник в случае неуплаты долгов подлежал аресту. Последствием излишней суровости норм Уложения стало то, что многие должники либо скрывались, либо договаривались с кредиторами о ведении дел вне судебных органов[1].

Теперь стоит перейти к этапам формирования института банкротства России. Стоит отметить, что уже в дореволюционный период в России вопросам конкурсного производства было уделено немало внимания.

Начинает формироваться институт несостоятельности, базирующейся на практике применения иностранного законодательства. Также по примеру римского права, взыскания обращались на личность должника. Последствием несостоятельности была продажа должника с торгов, распределение полученных средств между кредиторами: в первую очередь - долг князю, затем - иностранным кредиторам, а затем уже всем остальным. Также дореволюционный период отличителен интенсивными темпами развития конкурсного права и кодификацией. Первый кодифицированный акт - Устав о банкротах 1740 г. Следующие Банкротские уставы были приняты в 1753 г., 1763 г., 1768 г. В 1800 г. был издан Устав о банкротах. Наиболее разработанный - Устав о торговой несостоятельности 1832 г., который действовал до революции 1917 г. В 1884 г. был принят Закон «О порядке ликвидации дел частных и общественных установлений краткосрочного кредита», регулирующий вопросы несостоятельности банков и иных «кредитных установлений»[2].

После Октябрьской революции все дореволюционные акты были отменены. На их место пришло разъяснение Пленума Верховного Суда до 1927 года, после того, как в Гражданский кодекс РСФСР были включены нормы о несостоятельности гражданских и торговых товариществ и физических лиц. Но, не просуществовав и двух лет, разъяснения перестали применяться в результате свертывания НЭПа и постепенного исключения положений конкурсного права из советской правовой системы. Единым собственником имущества практически всех хозяйствующих на тот момент субъектов стало государство. В силу того, что значительно расширились торговые обороты страны, случаи несостоятельности стали достаточно распространенным явлением. В отличие от дореволюционной России вопросы неоплатности долгов решались не кредиторами, которые при новом режиме практически не имели никаких прав, а государством, так как теперь защищались никак не законные интересы кредиторов, а общий хозяйственный результат. В результате чего в течение многих лет убыточные предприятия существовали за счет государственного финансирования и периодического списания долгов.

---

[1] Федорова Г. В. Учет и анализ банкротств. Учебное пособие – 2-ое издание, - М.: Омега-Л, 2011. С. 12.

[2] Юлова Е.С. Конкурсное право: правовое регулирование несостоятельности (банкротства): учебное пособие, 3-е изд., переработанное и доп. / Е.С. Юлова. - М.: МГИУ, 2010. - 263 с.

Можно смело сказать, что до начала 90-х годов в России действовало огромное количество убыточных предприятий, полностью отсутствовала конкурентоспособная продукция, возникали злоупотребления со стороны руководителей предприятий, связанные, в том числе и с неосуществлением оплаты по договору.

После смены власти и начиная с 1992 года политика правительства России, была направлена на переход к рыночным отношениям. Этот период характеризуется сменой собственника большинства некогда бывших государственных предприятий в ходе их приватизации.

Понятие «рыночная экономика» под собой понимает становление и развитие предприятий различных организационно-правовых форм, основанных на разных видах собственности, а также появление новых собственников, как отдельных граждан, так и предприятий.

Большая часть предприятий в рамках рыночной экономики действуют на принципах состязательности. Обычно конкуренция поддерживается на государственном уровне, по причине того, что этот способ экономической организации позволяет использовать ресурсы национальной экономики наиболее выгодным и оптимальным образом. Менее эффективные предприятия, как правило, не выдерживают конкуренции и уходят с рынка.

Можно сказать, что такое явление, как банкротство – есть неизбежное явление рыночной экономики, которое работает как инструмент оздоровления экономики и способом согласования интересов всех участников товарообмена[1]. И в настоящее время задача механизма банкротства заключается в сохранении предприятия и собственности его владельца путем изменения системы управления предприятием.

ОСОБЕННОСТИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калашникова Н.А., студент
Научный руководитель: Шишкина Ю.С., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Ключевые слова: информационная безопасность, обеспечение информационной безопасности, Доктрина информационной безопасности РФ, угроза информационной безопасности РФ, средства обеспечения информационной безопасности.

Keywords: information security, information security, the Information Security Doctrine of the Russian Federation, the threat of information security of the Russian Federation, means of ensuring information security.

Аннотация: *в* статье рассматривается государственная политика обеспечения информационной безопасности в РФ, основные понятия и направления. Автор пытается определить особенность политики, для того чтобы, понять, чего в ней не хватает. В результате изучения, приходит к выводу, что в РФ нет конкретных программ для обеспечения информационной безопасности и их необходимо разрабатывать, но есть направления и методы.

Abstract: the article discusses the state policy of ensuring information security in the Russian Federation, the basic concepts and directions. The author tries to determine the peculiarity of the policy in order to understand what is missing in it. As a result of the study, it comes to the result that there are no specific programs in the Russian Federation to ensure information security and they need to be developed, but there are directions and methods.

Русская пословица говорит, кто владеет информацией – тот владеет миром и для нас это очень актуально. Информация в настоящее время играет важную роль в любой сфере, а развитие информационных технологий помогает эту информацию получать быстрее. Если раньше, чтобы раздобыть информацию, надо было шпионить, то сейчас достаточно уметь

[1] Федорова Г.В. Учет и анализ банкротств. Учебное пособие – 2-ое издание, - М.: Омега-Л, 2011. С. 15.

пользоваться компьютером на достаточно хорошем уровне. Полученная информация может быть вывернута и использована против любого человека и даже государства, поэтому необходимо защитить информацию. На законодательном уровне защитой информации занимается именно государство, оно обуславливает направление и принимает меры по обеспечению информационной безопасности.

Данная тема является очень актуальной, как в нашей стране, так и в других странах, потому что ежедневно на разные системы разных сфер жизни наносятся кибератаки и совершаются преступления с использованием компьютеров. По рейтингу стран после США Россия занимает второе место по атакам на сети. Проблема обеспечения защиты информации физической мерами состоит в том, что технологии, которые используются хакерами более совершенные, чем используемые для защиты, а только правовых мер порой не хватает.

Российское законодательство регулирует различные отношения, в том числе и отношения в области информационной безопасности. Основными видами отношений в данной области являются отношения:

– электронного документооборота, предпринимательской деятельности и торговли с использованием информационных отношений;

– обработки сведения, являющихся коммерческой, государственной и банковской тайной;

– в сфере обработки персональных данных.

На каждый вид этих отношений у нас в государстве есть закон, регулирующий их.

Основной для формирования государственной политики является Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 5 декабря 2016 года №646 (далее Доктрина). Доктрина представляет собой систему официальных взглядов и представляет собой документ стратегического планирования на обеспечение безопасности в информационной сфере.

Согласно Доктрине под информационной безопасностью следует понимать состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства; а под обеспечением информационной безопасности - осуществление взаимосвязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно- технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

В Доктрине указывается пять основных областей для обеспечения информационной безопасности:

1. обороны,
2. государственной и общественной безопасности,
3. экономической сферы,
4. область науки, образования и технологий,
5. область стратегической стабильности и равноправного стратегического партнерства.

В каждой из них описаны направления, в которых необходимо реализовывать различные мероприятия. Например, основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры и др.

В Доктрине указаны система, силы обеспечение информационной безопасности, но отсутствует конкретный план мероприятий по ее защите.

Таким образом, особенность нашей государственной политики в области обеспечения информационной безопасности является то, что в нашей стране нет определенных программ, которые показывали алгоритм действий и мер, а есть только законы, регулирующие порядок работы с разными видами документов. Проблема обеспечения информационной безопасности насущная во всем мире, я думаю, что против киберпреступлений бороться следует вместе.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации. - [Электронный ресурс] — Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

2. ИБ в России и в мире - https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ib-v-rossii-i-mire/

3. Обзор законодательства Российской Федерации в сфере информационной безопасности. [Электронный ресурс] — Режим доступа: https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/

4. Особенности государственной политики сша и россии в области обеспечения информационной безопасности – Малюк А.А., Савчик О.В.; [Электронный ресурс] — Режим доступа: https://cyberleninka.ru/article/v/osobennosti-gosudarstvennoy-politiki-ssha-i-rossii-v-oblasti-obespecheniya-informatsionnoy-bezopasnosti.

БЕЗОПАСНОСТЬ В ГОСУДАРСТВЕННО-ПРАВОВОЙ КОНЦЕПЦИИ Т. ГОББСА

Царьков И.И., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Обеспечение безопасности граждан, общества и государства в целом является ключевым фактором социальной жизни. В соответствии с иерархической теорией мотивации американского психолога А. Маслоу только мотив безопасности и реализация эффективных мер защиты, позволяет индивидам достигать иных, более высоких целей, нежели простое удовлетворение физиологических потребностей; осуществлять такие мотивы как общение, уважение в обществе и самореализация, которые дают возможность, как индивидуальному развитию, так и развитию общества.

Безопасность достигается, как политическими средствами, так и правовыми, но на протяжении долгого времени безопасность в большей мере относилась к сфере политики, которая допускала неопределенный перечень средств защиты, или, другими словами, оправдывались любые средства защиты. Первым кто существенно подорвал эту общую историческую установку, был английский просветитель, философ, теоретик права Т. Гоббс. По праву современные ученые называют великого англичанина создателем новой правовой теории, в которой центральным моментом является именно идея безопасности и вряд ли возможно аутентично уяснить смысл государственно-правовой теории Т. Гоббса, если не учитывать

это обстоятельство.

К сожалению, тексты Т. Гоббса дают повод читателю в несколько упрощенном понимании проблем безопасности и истолковать его теорию в старом традиционном духе, то есть в духе политической формулы римского императора Марка Аврелия – «Безопасность пчелы зависит от безопасности улья». Даная политическая формула устанавливает, что основные источники угроз индивидам и обществу исходят извне государства, а не находятся внутри общества и, таким образом, обеспечение внешней безопасности, – безопасности от врагов, - является приоритетной или даже единственной задачей государства. Вопрос о том, что внутренние угрозы не менее серьезные, нежели внешние и как внешние угрозы внутренние так же могут привести к утрате государственного суверенитета или вообще его существования, даже не поднимался.

Научной заслугой Т. Гоббса является его утверждение, что внутренние угрозы не менее опасны, чем внешние и, если не создать эффективных мер защиты индивидов от внутренних угроз, то невозможно будет достичь безопасности общества и от внешних. Таким образом, английской просветитель переворачивает традиционную политическую формулу Марка Аврелия и утверждает, что без защиты каждой отдельной пчелы невозможно защитить улей. Т. Гоббс был первым, кто перевел решение вопроса безопасности из сферы политики в сферу права.

Английская буржуазная революция и гражданская война, и те беды, которые выпали на долю англичан, очевидцем которых был Т. Гоббс, ярко демонстрировали, что при определенных обстоятельствах общество может саморазрушаться, то есть идти по пути хаоса и внешние угрозы в том не принимают никакого участия.

Научная гипотеза Т. Гоббса (в области политико-правового знания научную гипотезу принято называть «исходное положение») проста и в какой-то мере может показаться очевидной. Т. Гоббс утверждает, что индивиды являются независимыми, то есть предоставленными самим себе без какого-либо попечения, но не самодостаточными существами, что бы они не делали ради своего блага они не в состоянии этого достичь. (Что касается первой части гипотезы, то в эпоху Просвещения с Т. Гоббсом согласился бы любой ученый. Но, в отношении второй части гипотезы, - индивиды абсолютно не самодостаточны, - возникли серьезные сомнения, которые в наиболее ярой форме изложил младший соотечественник Т. Гоббса – Дж. Локк. Дж. Локк согласен, что индивиды должны быть предоставлены самим себе и принимать решения о своем благе на свой страх и риск, но индивиды не абсолютно не самодостаточны, а относительно. Эта маленькая поправка в гипотезе привела к самым существенным спорам, как по поводу эффективных мер защиты, так и в общей теории государства и права).

Смысл научной гипотезы Т. Гоббса заключатся в том, что прежде чем определять правовые нормы, гарантирующие безопасность каждого отдельного индивида, необходимо выявить обстоятельства, препятствующие достижению этой цели. Таким обстоятельством для Т. Гоббса являться то, что в исходном положении каждый индивид имеет право самостоятельно заботиться о средствах свой индивидуальной защиты, то есть защиты своей жизни и собственности. Такое состояние общества Т. Гоббс называет «естественным состоянием». Термин «естественное» Т. Гоббс использует в значении человеческих природных инстинктов, но не разумного поведения людей. Первичными (природными) инстинктами он считает удовлетворение физиологических потребностей и инстинкт самосохранения. Самый главный вывод, который делает английский философ, заключается в том, что как первый инстинкт, так и второй норм (правил поведения) не порождают. Если каждому индивиду предоставляется право на жизнь (имеется в виду простого биологического существования, когда человек заботится о пропитании) и право самостоятельно заботиться о средствах своей индивидуальной защиты, что бы выжить, то результатом оказывается не уверенность в самосохранении, а прямо противоположный результат – самоуничтожение. Такое естественное состояние он называл - «Война каждого против каждого». Как бы отдельный индивид не был уверен в своих личных возможностях и силе в вопросе самосохранении, гарантий на выживание нет.

На одного сильного и умного может найтись тысяча слабых и глупых. (Это положение перекликается с, упомянутой выше, иерархической теорией мотивации А. Маслоу. Последний также был убежден, что если человек озабочен исключительно удовлетворением своих физиологических потребностей, - потребности не удовлетворены, - то и мотив безопасности не возникнет).

Таким образом, вопрос безопасности не решается на основании инстинктов (силы), а решается на основании разума – взаимного общественного согласия. Такое согласие Т. Гоббс называет «Общественный договор» в соответствии, с которым каждый индивид обязан отказаться от решения вопросов своей личной безопасности и безопасности своей собственности. «Общественный договор» учреждает (создает) государство (по терминологии Т. Гоббса «Левиафана»), которое с момента учреждения приобретает исключительное право устанавливать правила поведения и контролировать их исполнение всеми законными средствами.

Сам английский просветитель называет государство («Левиафана») смертным Богом на земле. Эта метафора отражает суть гоббсовской государственно-правовой концепции. В религиозной традиции Бог является высшей нормативной инстанцией, которая обладает возможностью из НИЧТО создать НЕЧТО. В сфере человеческих отношение именно государство занимает место Бога, поскольку из НИЧТО, - отсутствия каких либо норм в естественном состоянии, - создает НЕЧТО – правила поведения.

Впоследствии именно данное положение вызвало у представителей правового сообщества массу критических замечаний и упрощенное понимания смысла гоббсовской государственно-правовой теории. Главное обвинение выражалось в чрезмерном доверии к государству в вопросах индивидуальной защиты (определения средств защиты) и отсутствия правовых гарантий от того, что сам «Левиафан» не будет провоцировать «Войну каждого против каждого».

Напомним, что именно вопрос безопасности каждого отдельно индивида, эффективных мер защиты от внутренних угроз, являлся для Т. Гоббса камнем преткновения. Для него самым важным было создание таких политико-правовых условий, при которых невозможна гражданская война. Поэтому, он четко формулирует цели и задачи государства. Государство учреждено и имеет право устанавливать правила поведения и контролировать их исполнение всеми законными средствами, но только при одном условии – условии, если все его средства будут направлены на защиту жизни и собственности своих собственных граждан. По сути, это и есть содержание Общественного договора Т. Гоббса.

Критика государственно-правовой концепции Т. Гоббса в чрезмерном доверии государства была бы оправдана, если бы не еще одно обстоятельство. Отвечая на замечание своих оппонентов в чрезвычайной сложности его государственно-правой теории (теории Общественного договора) для понимания простыми гражданами, он отвечал, что данный аргумент, - граждане просты и не образованы, - используется бандитами и политическими проходимцами, для которых цель политического господства – извлечение личной выгоды, а не общее благо государства. Истинный «Левиафан» обязан проводить просветительскую политику, разъясняя гражданам их личную выгоду от полного повиновения правилам поведения, установленных государством. «Левиафан» (государство) обязано разъяснять гражданам их истинные обязанности и истинные обязанности перед ними государства. По сути дела, фактом Общественного договора и учреждения государства, для английского просветителя является позиционирование государства как правовое государство, у которого нет иных забот, кроме заботы о безопасности людей, а все, что свыше этого, то это по мере возможности.

В силу этих посылок Т. Гоббс делает один из основных своих теоретико-практических выводов, утверждая, что никакое неудобство, исходящее от буквы закона не может оправдать решение, идущее в разрез с законом. Превыше всего Закон государства, именно он защищает индивидов от внутренних угроз. Иная ситуация возвращает общество в естественное состояние – состояние неопределенности и даже хаоса. Закон государства должен четко и ясно определять, что можно, а что запрещено совершать субъектам права. Тем не менее, Закон государства не совершенен, но он наименьшее зло, нежели неповиновение Закону.

Защита граждан от внутренних угроз выстраивается на основании строго соблюдения гражданами законов государства. Они должны быть ясными и понятными для любого, даже для не образованного человека. Поэтому, если Закон не определяет некое действие как преступное, то оно не может осуждаться юридически – нет Закона, нет преступления. Это утверждение в настоящее время является самым распространенным убеждением и мало кто из современных юристов его оспаривает. Причинение вреда индивидам определяется исключительно посредством Закона.

Несомненно, позитивная выгода данной правовой формулы очевидна, она исключает возможность самосуда, возможность того, что ююбой индивид самостоятельно будет определять причиненный ему вред и самостоятельно карать «преступника». Последнее, по мнению Т. Гоббса, и есть наибольшее зло для государства, которое ведет к его уничтожению. Государство – смертный Бог на земле; Бог, но смертный. Государство может быть уничтожено усилиями своих собственных граждан.

При всей позитивной выгоде правовой формулы – нет Закона, нет преступления, тем не менее, ее ограниченность, так же очевидна. Нет Закона, нет преступления, но в таком случае можно поставить вопрос: «Если нет закона, возможна судебная защита?» С точки зрения логики гоббсовской государственно-правовой теории, защита невозможна. Даже, если индивиду реально причинен вред, но данные действия не предусмотрены законом как преступные деяния, то рассчитывать на законную судебную защиту он не в праве, иск будет отклонен.

Библиографический список

1. Аврелий, М. Размышления. М., 2008.
2. Гоббс, Т. Соб. соч. в 2-х т. М., 1964.
3. Локк, Дж. Соб. соч. в 3-х т. М., 1985.
4. Царьков, И.И. Развитие правопонимания в европейской традиции права. СПб., 2006.

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ КАК ОДИН ИЗ ФАКТОРОВ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Якушин В.А., д. ю. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Ключевые слова: факторы обеспечения национальной безопасности; политическая система, её элементы и средства реализации их нормативных предписаний; предупреждение преступлений и иных правонарушений; субъекты предупредительной деятельности; система субъектов предупредительной деятельности.

Аннотация: обеспечение национальной безопасности гарантирует само существование любого государства, его суверенитета и успешного развития общества. Вот почему вопросам национальной безопасности уделялось и уделяется столь пристальное внимание ученых различных сфер науки – философов и политологов, социологов и психологов, медиков и юристов и т.д.

В последние годы проблемам национальной безопасности стали уделять больше внимания в сфере юриспруденции и особенно её криминалистического направления, поскольку состояние преступности напрямую связано с вопросами обеспечения национальной безопасности. В данной статье сделана попытка осмысления некоторых проблем, влияющих на преступность, её снижение и предупреждение.

Национальная безопасность любого государства, в том числе и России, зависит от множества факторов – экономики, политики, социального устройства и т.д.

Вместе с тем, национальная безопасность России имеет и должна иметь и специфические факторы её обеспечения. Это связано с рядом как объективных, так и субъективных об-

стоятельств.

К объективным обстоятельствам можно отнести наличие огромной территории страны, колоссальные запасы природных ресурсов и при этом малую плотность населения на квадратный километр. С одной стороны, просторы родины и запасы её природных ресурсов есть гаранты национальной безопасности. А с другой стороны – много желающих воспользоваться подобной ситуацией и пограбить эти ресурсы.

В этих условиях наибольшую значимость приобретают субъективные факторы обеспечения национальной безопасности – характер и способы производства, распределения и перераспределения продуктов труда, устройство политической системы в нашей стране. В свою очередь эффективность работы всей политической системы зависит от средств обеспечения и реализации нормативных предписаний каждого из звеньев нашей политической системы – государства, общественных, партийных и самодеятельных организаций, трудовых коллективов. Если эти средства, инструменты этих звеньев политической системы скоординированы, то они приносят положительные результаты, в том числе и по обеспечению национальной безопасности в том или ином её сегменте.

Одним из этих сегментов, направлений, обеспечивающих национальную безопасность, является фактор снижения уровня преступности в стране. А он достигается, прежде всего, за счет осуществления профилактической, предупредительной деятельности всех звеньев политической системы. Чем ниже уровень преступности, тем выше уровень национальной безопасности. Недопущение роста преступности, а тем более формирования на этой основе специфической преступной субкультуры, для нашей страны с её огромными, порой труднодоступными регионами – настоятельное веление времени – это залог обеспечения национальной безопасности в этом направлении. А основное средство борьбы с преступностью – это её предупреждение. Как тут не вспомнить мысль Ч. Беккариа и Монтескье об умном законодателе, который вместо того, чтобы карать за совершенное преступление, подумает, как его предотвратить.

В последние десятилетия в России, после распада СССР это особенно ясно видно, канула в лету система предупреждения преступлений. Это объясняется рядом причин.

Во-первых, в настоящее время ни в научной, ни в политической среде нет четкого понимания, как соотносятся понятия «субъекты предупреждения преступлений и правонарушений», «правоохранительные органы» и «органы по охране общественного порядка». Эти понятия почему-то начали отождествлять, а в силу этого многие субъекты социальной действительности просто взяли и «исключили» себя из системы не только предупредительных органов, но и системы субъектов правоохранительной деятельности.

Все реально свелось к тому, что есть по охране общественного порядка. Они и только они и должны заниматься предупреждением (профилактикой) правонарушений и преступлений. Правда органы власти и МВД требуют, чтобы в организациях принимались меры по борьбе с курением, пьянством и наркоманией - создавались комиссии, наглядная информация и др.

Во вторых, сейчас нет самой этой четко определенной системы субъектов, которые могут и должны заниматься предупреждением преступлений.

В-третьих, исчез тот орган, на который в масштабах страны возлагалась бы обязанность координации предупредительной деятельности различных органов и организаций России.

В-четвертых, политические органы страны за последние десятилетия ни одного раза не «били в набат» об этом комплексном направлении деятельности государства и общества. Ими поднимаются проблемы лишь по отдельным направлениям борьбы с преступностью – терроризмом, наркотиками, коррупцией. Остальные виды преступлений остаются без надлежащего внимания.

В рамках небольшой статьи хотелось бы остановиться на рассмотрении этих четырех обстоятельствах. Прежде всего, надо на законодательном уровне определить то, что в систему правоохранительных органов государства входят не только все силовые структуры – МВД, ФСБ, Министерство обороны, МЧС и др., но и вся судебная система. Да-да, именно

суды стоят на страже охраны, защиты прав граждан, организаций и государства. Вся судебная система этому служит и должна служить. Иначе весь смысл правосудия исчезает. Более того, в ч. 2 ст. 43 УК РФ подчеркивается, что целями наказания, назначаемого судом, является и цель предупреждения преступлений. Анализ норм ч.ч. 1 и 2 ст. 2 УК РФ позволяет сделать вывод о том, что и при применении иных мер уголовно-правового воздействия суды должны решать задачу предупреждения преступлений. Из анализа их применения суды должны (что сейчас не делают) давать своё заключение об эффективности этих мер.

Представляется, что на нормативном уровне должна быть определена система субъектов предупредительной деятельности. Помимо правоохранительных органов (включая суды) должны быть определены:

а) иные государственные и муниципальные органы, на которые бы возлагалась задача (наряду с их основными задачами) по предупреждению преступлений и правонарушений и

б) иные субъекты социальной действительности, которые в силу характера их деятельности должны заниматься предупредительной деятельностью. Это, например, добровольные народные дружины (ДНД), структуры народного фронта и общественных фондов, общественные советы при выборных органах и силовых структурах и т.п.

Нужно срочно определиться с тем органом, который бы на деле координировал работу всех субъектов, занимающихся предупреждением преступлений и правонарушений. Ранее эта функция была возложена на прокуратуру России. Сейчас в связи с тем, что у неё «отобрали» реальные рычаги влияния на это направление деятельности и превратили, по сути, в органы народного контроля, она не может этого делать. Восстановить полномочия прокуратуры означает возвратить ей полномочия по наведению и в этой сфере.

Предупреждение преступлений и иных правонарушений есть залог формирования у населения страны законопослушания, а значит и залог не совершения не только «бытовых» преступлений и правонарушений, но и особо тяжких и особо опасных преступлений – терроризма, захвата заложников, создания организованных преступных групп и др.

Но есть ещё один очень важный аспект предупреждения преступлений и правонарушений – это сохранение тесной связи законопослушного поведения с нормами морали и нравственности. Её разрушение ведет к необратимым процессам – в конечном итоге к развалу не только законности, но и нравственной деградации народа, а потом и страны. Например, уличные шествия голых людей в некоторых западных странах уже не преступления, связанные с исключительным цинизмом и дерзостью по отношению к другим людям, и особенно к детям, а нормальное проявление свободы. Это же сплошное попустительство преступлению против интересов ***человеческого*** образа жизни. Это уже не просто угроза обществу от преступлений, а угроза национальной безопасности государства.

Разумеется, что я лишь в общих чертах затронул значение предупредительной деятельности обеспечения национальной безопасности. Эта большая и комплексная проблема, которая требует внимания и усилий не только научной общественности, но и политических, государственных и религиозных структур.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017) [Текст] // Собр. законодательства РФ.

2. Теоретические основы предупреждения преступности / В.В. Клочков, А.С. Шляпочников, В.Н. Кудрявцев и др.; Отв. ред.В. К. Звирбуль и др.; Всесоюзн. ин-т по изучению причин и разработке мер предупреждения преступности. - М.: Юрид. лит., 1977. -256 с.

НЕКОТОРЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЗДРАВООХРАНЕНИЯ В РФ

Якушина Л.Н., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

В 2014 году был принят Федеральный закон "О стратегическом планировании в Российской Федерации"[1], а в 2015 году подписан Указ Президента РФ "О Стратегии национальной безопасности Российской Федерации" (далее по тексту – Стратегия или Указ Президента)[2].

Согласно п. 1 Указа Президента Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

Национальная безопасность определена в п. 6 Указа Президента как состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;

В Указе Президента констатируется, что в решении задач укрепления здоровья граждан «наметились позитивные тенденции. Отмечаются естественный прирост населения, увеличение средней продолжительности жизни» (п. 10 Стратегии).

Тем самым, здоровье граждан России, демографическая ситуация в стране безусловно, являются важнейшими показателями состояния национальной безопасности. Именно поэтому в Указе Президента в качестве национального интереса названы повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны. Осторожная констатация факта того, что в России только лишь «наметились позитивные тенденции» в сфере укрепления здоровья граждан, позволяют говорить о том, что в этой сфере для России существует большой потенциал, - как для работы непосредственно всей отрасли медицины и здравоохранения, так и самого законодателя, целью которого будет создание таких правовых основ, которые позволят российской медицине перейти на качественно более высокий уровень.

Факторами, негативно влияющими на национальную безопасность в сфере охраны здоровья граждан, в Стратегии (п. 73) называются: недостатки в реализации государственной политики в сфере охраны здоровья граждан в части, касающейся обеспечения доступности медицинской помощи и реализации гарантий ее оказания населению, несовершенство действующей системы медицинского страхования, недостаточное финансирование системы высокотехнологичной медицинской помощи и низкий уровень квалификации медицинских работников, не полностью сформированная нормативно-правовая база в указанной сфере.

В настоящей работе хотелось бы остановиться только на нескольких из указанных проблем.

---

[1] Федеральный закон от 28.06.2014 N 172-ФЗ (ред. от 31.12.2017) "О стратегическом планировании в Российской Федерации"

[2] Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации"

Известно, что здоровье нации определяется здоровьем каждого человека определенного общества. Состояние здоровья человека, в первую очередь, определяется его личным отношением к своему здоровью, и только во вторую очередь – системой здравоохранения и качеством лечения.

Огромная разница в продолжительность жизни мужчин и женщин в России заставляет задуматься о разных психологических подходах к состоянию своего здоровья в зависимости от гендерных признаков. По состоянию на 2017 год средняя продолжительность жизни женщины в России составляет 77 лет, а мужчины – 66,5 лет, что на 10,5 лет меньше чем у женщин[1]. Такая разница в продолжительности жизни во многом обусловлена отношением человека к собственному здоровье, но это отношение, в рамках государственной политики, нельзя рассматривать как личное дело каждого. При этом здоровье нации, должно определяться именно формированием должного отношения каждого человека к своему здоровью.

Так, проводимые исследования[2] показывают, что более 30% мужчин остаются на работе, чувствуя недомогание, и более 35% продолжают рабочий процесс при наличии плохого самочувствия и повышенной температуры. Данный факт характеризует не только сформировавшийся стереотип поведения – рисковать своим здоровьем ради работы, но и рисковать здоровьем окружающих ради работы. Такой «мнимый героизм», как правило, в российском обществе или не оценивается вообще, либо считается нормой. И только малая часть населения сможет дать понять больному человеку, что общением с ним, под угрозу ставиться здоровье неограниченного количества лиц.

Полагаем, что в России, на уровне политики укрепления здоровья нации необходимо закрепление и планомерное проведение пропаганды и стимуляции граждан России к ведению здорового образа жизни и профилактики заболеваний. Данный фактор редко рассматривается как угроза здоровью нации, на наш взгляд, именно из-за обывательского мнения, сводящегося к тому, что система здравоохранения нужна только для того чтобы лечить. На самом же деле – здоровье человека должно начинаться с профилактики заболеваний, ведения здорового образа жизни, периодических прохождений медицинского осмотра. С этой точки зрения, большой интерес представляет статья С.И. Нестеровой[3], которая утверждает, что «результативным способом заставить людей обращать внимание на свое здоровье стала бы дифференцированная шкала по налогу на доходы физических лиц в зависимости от того, как часто человек обращается за лечением в лечебно-профилактические учреждения по аналогии с дифференцированной шкалой страхования автомобилей. Так, например, если в течение года человек ни разу не брал больничный и при этом прошел все необходимые превентивные мероприятия, на следующий год ставка налога на доходы физических лиц для него должна быть понижена на 0,25%». Можно предположить, что бережное отношение к своему здоровью должно воспитываться в человеке еще с раннего детства. Наилучшим способом воспитания ребенка в целях ведения здорового образа жизни, безусловно, должен являться образец поведения его родителей. Но для того, чтобы преломить ситуацию «наследственного» безалаберного отношения российских граждан к своему здоровью, законодателю бы следовало подумать об уроках здоровья в российской системе образования, начинать которые, по нашему мнению, надо еще в дошкольных учреждениях.

Второй вопрос, который хотелось бы затронуть в настоящей статье – это вопрос, возникший в сравнительно недавний период времени, но остро нуждающийся в правовом регулировании – определение статуса эмбриона человека, находящегося в состоянии криоконсервации.

Известно, что эмбрион «в пробирке» фактически оторван от организма матери, а физически находится в медицинском учреждении. При этом, возможность его имплантации ста-

---

[1] www.reconomica. ru› средняя-продолжительность-жизни-в-рф.

[2] Акимов А.Н., Смазнов В.Ю. Отношение к своему здоровью мужчин городской открытой популяции в зависимости от возраста// Омский научный вестник, № 4, 2015. С. 282-284.

[3] Нестерова С.И. Здоровье без денег – миссия невыполнима? // Вестник Омского университета. Серия «Экономика». 2015. №м 3. С. 358-365. 363 с.

виться в зависимость от воли как минимум двух лиц (исключение составляет случай, когда одинокая женщина прибегает к методам вспомогательной репродукции) – будущих мамы и папы. В судебной практике возникает все больше и больше споров между бывшими супругами (сожителями), которые пробуют разделить эмбрионы, запретить их использование после развода, уничтожить. При этом, Закон не устанавливает никаких правил, на основе которых могли бы решаться эти вопросы в судебном или досудебном порядке. Единственными регуляторами таких правоотношений становятся медицинские клиники, которые руководствуясь только собственным опытом и Приказом Минздрава РФ № 107н[1] разрабатывают свои проекты договоров криоконсервации эмбрионов. Считаем, что подобный пробел в праве просто не допустим. Наиболее очевидным является недостаток правового регулирования в вопросе о возможности отзыва согласия на имплантацию эмбриона. В мировой практике существует два диаметрально противоположным подходам:

1. Возможность отзыва согласия на хранение и имплантацию эмбриона в любой момент до имплантации (как было в деле Эванс против Соединенного королевства). Подобное положение предусмотрено законодательствами Дании, Франции, Греции, Нидерландов и Швейцарии.

2. Невозможность отзыва согласия на хранение и имплантацию эмбриона после оплодотворения (после создания эмбриона в пробирке) – установлено в законодательствах Австрии, Эстонии[2].

И если первый подход обусловлен исключительно личной свободой каждого определять свое желание стать родителем, то для доказательства логичности второго подхода очень подходит яркий пример, приводимый судьей ЕСПЧ от России Д.И. Дедовым, который говорит следующее: если «бывший муж не может потребовать аборта, когда ребенок начал развиваться внутри матери, так почему же эмбрион (в пробирке) не имеет таких же прав на жизнь, как и плод внутри матери?»[3].

В заключении хочется согласиться с законодателем в том, что в России «наметились позитивные тенденции» в сфере здравоохранения. Но, в то же время остается множество вопросов, которые требуют незамедлительного правового регулирования. Конечно же, это касается значительно большего круга вопросов, нежели были затронуты в настоящей статье. К ним можно отнести и недостаточное финансирование системы здравоохранения и отсутствие исчерпывающего правового регулирования вопросов трансплантологии (в том числе и посмертной) и отсутствие прозрачного правового регулирования возможности или невозможности проведения исследований с участием человеческих половых клеток, что в потенциале своем, могло бы существенно продвинуть отечественную медицину и фармацию на более высокий качественный уровень и продвинуть ее на международном рынке медицинских услуг.

[1] Приказ Минздрава России N 307н, РАН N 4 от 04.06.2015 (ред. от 01.12.2017) "Об утверждении перечня учреждений здравоохранения, осуществляющих забор, заготовку и трансплантацию органов и (или) тканей человека" (Зарегистрировано в Минюсте России 18.06.2015 N 37705).

[2] См.: Отчет о проведении исследования. Проблемы биоэтики Европейского суда по правам человека. //www.echr.coe.int/Documents/Reserch)report_bioethics_RUS.pdf (дата обращения 05.01.2018).

[3] Д.И. Дедов (судья ЕСПЧ) «Начало жизни: от Эванса до Паррилло»// Российский ежегодник Европейской конвенции по правам человека (выпуск 2) «статут», 2016. СПС «Консультант Плюс».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ КОНТЕНТОМ

Горбатов Н., Веселов В., студенты
Научный руководитель: Федосеева О.Ю., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Развитие веб-технологий и дизайна нарастает быстрыми темпами, появляются новые инструменты и стандарты для разработчиков, ориентация на которые является обязательной при создании качественного проекта. Открывается много фирм, каждая из которых нуждается в сайте.

История создания сайтов берет свое начало с 90-х годов прошлого столетия и тесно связана с возникновением сети Интернет. Первопроходцем в этой сфере был женевский ученый из Европейской лаборатории элементарных частиц Тим Бернерс-Ли. Именно он является создателем первого в мире сайта. Но еще до него в далеких сороковых годах прошлого столетия Ваннервар Буш развивал идею о том, что благодаря специальным техническим устройствам можно расширить человеческую память и проиндексировать накопленную веками информацию. Это давало бы возможность, по его мнению, организовать быстрый поиск необходимой информации. Именно такой принцип и лежит в основе сегодняшних сайтов.

Сайту надо где-то жить – это несомненный факт и поэтому нам надо позаботиться о проблеме размещения сайта, сведения о хостинге становятся просто жизненно необходимыми.

Хостинг – это понятие, которое определяет место жительства сайта в Интернете. Хостинг обеспечивает необходимое пространство для хранения сайта в Интернете.

Если сайт будет просто существовать у нас на компьютере, то никто, кроме нас и наших знакомых его не увидит. Следовательно, нужно искать новые нивы, на которых можно расположить наше творение.

Хостинг – это понятие арендуемое, то есть, нельзя приобрести его навсегда, вы должны периодически выплачивать за него определенную сумму. К примеру, минимальный срок заказа хостинга – один месяц. Но давайте углубимся в рассмотрение этих значений, чтобы вам всё стало ясно.

Хостинг – это как бы квартира для сайта. То есть, вы обращаетесь к какому – то хостинг провайдеру, он предлагает вам определенные условия (виртуальный или выделенный сервер, поддержка скриптов и языков, необходимое пространство), а вы решаете, подходят ли они вам.

После согласия вам выдается заказанное место на жестком диске, это и есть ваша квартира. Сам жесткий диск – это часть сервера провайдера, все сервера хранятся в специально организованных зданиях, которые именуются дата-центрами. Здесь всё обусловлено для того, чтобы всё оборудование находилось в непрерывной связи с Интернетом. Соответственно, ваш сайт, хранимый на харде одного из серверов, также расположен в Виртуальной Паутине.

Широкий спектр выбора хостинга для размещения сайта может легко запутать. Существует множество аспектов, которые нужно рассматривать и сравнивать. На некоторых хостингах очень много технических деталей, которые могут быть не совсем понятными. В этом случае невозможно определится, понадобятся ли некоторые функции или вообще неизвестно их назначение.

Наш выбор остановился на бесплатном хостинге Beget.

Система управления контентом или CMS (англ. аббр. от Content Management System) – программное обеспечение, предназначенное для создания, организации структуры, редактирования и управления веб-сайтом. Другими словами это движок сайта.

Пользователю сети Интернет не видно, что происходит внутри сайта, который он посещает. Но только web-разработчикам и их заказчикам известно, что большинство современных веб-сайтов строятся на основе выше упомянутых систем.

Принцип работы. CMS-движки дают возможность добавлять и редактировать контент сайта, не изменяя внутренний механизм организации и вывода страниц. Условно CMS разделена на два хранилища информации: для баз данных с контентом страниц и элементов визуализации, позволяющих показывать содержимое сайта посетителям (графические элементы, шаблоны и т.д.).

Для удобной работы с информационным наполнением сайта большинство движков имеют инструменты визуального редактора (WYSIWYG) — программу, которая создает HTML-код из облегчающей пользовательское форматирование текста разметки. Поэтому в процессе работы с текстом сразу виден конечный результат.

Цели использования. CMS предназначена для самостоятельного наполнения сайта контентом без привлечения технических специалистов. Чтобы использовать движок специальные знания программирования и веб-технологий, как правило, не нужны (но для работы с системой управления сайтом требуется освоить ее принципы и детально изучить руководство по эксплуатации CMS).

История возникновения. Первые CMS появились в начале 2000 года, но в то время они были очень узконаправленными решениями и в основном решали задачу управления одним сайтом, немного позднее CMS стали выполняться в более универсальном виде, то есть с возможностью подстройки под конкретный проект. Эволюция CMS происходит достаточно быстро, и это в первую очередь связано с появлением новых течений и стандартов, например, появление методики AJAX на текущий момент дает возможность представить интерфейс CMS практически неотличимым по интерактивности от обычных desktop-приложений. Выбор CMS под конкретный Интернет-сайт вопрос нелегкий, но решаемый. Все CMS условно можно разделить на коммерческие и бесплатные. Разберем преимущества и недостатки бесплатных CMS.

Преимущества бесплатных CMS:

- Очень большое количество компаний, а особенно фрилансеров, занимающихся разработкой и оказывающих техническую поддержку;
- достаточно высокая функциональность;
- большие возможности по расширяемости, большое количество бесплатных дополнений и модулей;
- средняя надежность базовой версии системы;
- нет жестких требований к хостингу;
- отсутствие платы за систему.

Недостатки бесплатных CMS:

- отсутствие официальной технической поддержки, невозможность формально урегулировать конфликтные ситуации;
- техническую поддержку преимущественно осуществляют сторонние разработчики, которые в основной своей массе об особенностях и возможностях CMS знают, основываясь на опыте изготовления собственного сайта;
- функциональность хуже, чем у платных систем;
- расширяемость высокая, но часто после внесения каких-либо изменений в систему корректно обновить её будет невозможно;
- как и многие популярные проекты с открытым исходным кодом, базовые версии CMS-систем надёжны, но на практике их функционал необходимо расширять дополнительными модулями, код которых тоже открыт и может быть доступен злоумышленнику, а вот разработчиков, проверивших его на безопасность, недостаточно. Поэтому, в целом бесплатная CMS с дополненным функционалом, будет незащищена от хакеров. Это усугубляется тем, что бесплатные системы очень уязвимы к неосторожным действиям пользователей;
- для настройки системы пользователь должен обладать достаточной технической ква-

лификацией: знанием html, основами программирования и работы с БД. Бесплатные системы созданы программистами для программистов, за счёт этого они и развиваются;

- редко можно найти бесплатную CMS с хоть какой-нибудь документацией, не говоря уже об инструкциях пользователя и разработчика.

О Wordpress и сравнение с его аналогами

На WordPress работает 23% всех сайтов в интернете, но это не единственная бесплатная система управления контентом. Существуют и другие платформы, такие как Joomla и Drupal. Но каждая из них имеет свои плюсы и минусы. Сейчас мы сравним Drupal, WordPress или Joomla, чтобы выяснить, какая из этих систем является лучшей.

Все три популярных CMS имеют много общего с точки зрения технологии, философии и сообщества.

Joomla, Drupal, WordPress являются бесплатным программным обеспечением с открытым исходным кодом. Все три написаны на PHP.

Все три используют MySQL в качестве СУБД. WordPress поддерживает только MySQL, в то время как Joomla и Drupal поддерживают другие системы управления базами данных.

Все три используют темы и шаблоны для визуального оформления сайтов и подключаемые плагины, модули для расширения функционала.

В качестве программного обеспечения с открытым исходным кодом, все они являются проектами, развиваемыми и поддерживаемыми сообществом.

Но в ряде аспектов эти системы отличаются друг от друга. У них разная концепция относительно того, что включать в ядро платформы, как обрабатывать модули и шаблоны, как обеспечивать безопасность и т.д.

Рассмотрим, чем отличаются WordPress, Joomla и Drupal по безопасности.

Безопасность является важным фактором при выборе CMS для сайта.

Так как WordPress является самой популярной CMS в мире, то сайты, работающие на базе этой платформы, часто становятся мишенью для хакеров. Тем не менее, WordPress построен на безопасном коде, и он быстро реагирует на уязвимости в системе. WordPress также имеет механизм автоматического обновления, который позволяет обновлять платформу, когда появляется исправление системы безопасности.

Сайты, работающие на базе WordPress, могут быть дополнительно оснащены системой автоматического создания резервных копий, двухфакторной аутентификации, а также другими продвинутыми технологиями.

Также существует встроенный механизм, который сообщает о появлении обновлений для тем и плагинов WordPress. Это позволяет быстро реагировать на любые уязвимости в системе безопасности.

В вопросах безопасности отличия Joomla от WordPress минимальны. Платформа оперативно реагирует на любые уязвимости в системе и очень быстро исправляет их. В то же время поддержка сайта и установка обновлений все также остается слабее, чем в WordPress.

Существуют расширения, предназначенные для резервного копирования сайта, работающего на базе CMS Joomla. Вы также можете усилить безопасность сайта, применив те же передовые практики, что и для WordPress.

Drupal серьезно относится к безопасности. Разработчики публикуют информацию об обнаружении и устранении уязвимостей. Существует мнение, что Drupal является более безопасной платформой, потому что мы не так часто слышим о взломе сайтов на Drupal. Но это связано с тем, что Drupal не так популярен, как Joomla или WordPress.

Сравнивая Drupal, Joomla и WordPress — все три платформы соответствуют современным стандартам безопасности.

И Drupal, и Joomla, и WordPress являются надежными системами управления контентом. Drupal и Joomla по умолчанию поставляются с большим количеством встроенных функций, чем WordPress. Тем не менее, WordPress «бьет» их простотой в использовании, большим количеством плагинов и тем, а также более развитым сообществом. Мы считаем, что большинству пользователей будет намного проще работать с WordPress, нежели с Joomla или Drupal.

Для примера создания сайта мы выбрали платформу WordPress.

Таблица 1 – Сравнительная характеристика Drupal, Joomla и WordPress

CMS/Характеристики	**DRUPAL**	**Joomla**	**WordPress**
Простота использования	Drupal наиболее требователен к технической осведомленности пользователя, что окупается самыми широкими возможностями при создании сайтов. От версии к версии наблюдается некоторое упрощение Drupal, но даже это не делает систему лучшим выбором для нежелающих глубоко изучать систему и тратить деньги на специалиста	Проще Drupal, сложнее WordPress. Относительно не напрягающая установка и настройка в совокупности с нетребовательностью к затратам времени на понимание структуры и терминологии дают возможность самостоятельно построить весьма сложный сайт	Технические знания в данном случае совсем не обязательны. WordPress простая и интуитивная. С ее помощью можно чрезвычайно быстро создать простой сайт. Также WordPress привлекает возможностью без труда переносить текст из текстовых документов на сайт, чем не могут похвастать Drupal и Joomla
Темы **плагины**	> 1800 > 7000	> 1000 > 32000	> 2000 > 45000
Безопасность	Drupal серьезно относится к безопасности. Разработчики публикуют информацию об обнаружении и устранении уязвимостей.	В вопросах безопасности отличия Joomla От WordPress минимальны. Платформа оперативно реагирует на любые уязвимости в системе и очень быстро исправляет их. В то же время поддержка сайта и установка обновлений все также остается слабее, чем в WordPress.	WordPress является самой популярной CMS в мире. Сайты, работающие на базе этой платформы, часто становятся мишенью для хакеров. Тем не менее, WordPress построен на безопасном коде, и он быстро реагирует на уязвимости в системе.

Вывод

В статье мы сравнили на безопасность наиболее распространенные платформы для создания своего сайта, привели их достоинства и недостатки, по которым вы сможете выбрать для себя удобную платформу для создания своего сайта.

Библиографический список

1. «WordPress vs Joomla vs Drupal – что лучше?» [Электронный ресурс] — Режим доступа: http://www.internet-technologies.ru/articles/wordpress-vs-joomla-vs-drupal-chto-luchshe.html
2. «Веб-дизайн умирает или шансы еще есть?» [Электронный ресурс] — Режим доступа: https://lpgenerator.ru/blog/2016/03/18/veb-dizajn-umiraet-ili-shansy-eshe-est/
3. «История развития веб сайтов (web разработки)» [Электронный ресурс] — Режим доступа: http://preal.ru/webhist/istoriya-razvitiya-veb-saytov-web-razrabotki/
4. «Что такое хостинг и домен»[Электронный ресурс] — Режим доступа: http://service-joomla.ru/ kak-sozdat-svoy-sayt/item/5-chto-takoe-chosting-i-domen.html
5. «История возникновения CMS» [Электронный ресурс] — Режим доступа: https://promo.ingate.ru/ seo-wikipedia/cms/
6. «Система управления сайтом (CMS)» [Электронный ресурс] — Режим доступа: http://www.grizliart.ru/cms/
7. «WordPress vs Joomla vs Drupal: CMS Руководство по сравнению» [Электронный ресурс] — Режим доступа: https://business.tutsplus.com/ru/articles/wordpress-vs-joomla-vs-drupal-cms-comparison-guide--cms-26581
8. «Какую CMSвыбрать для сайта: сравнение WordPress, Joomla и Drupal» [Электронный ресурс] — Режим доступа: https://lifehacker.ru/2014/06/16/kakuyu-cms-vybrat-dlya-sajta-sravnenie-wordpress-joomla-i-drupal/

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В АСПЕКТЕ ГРАЖДАНСКО-ПРАВОВЫХ ОТНОШЕНИЙ

Краснов С.С., инженер
Волжский университет имени В.Н. Татищева
г. Тольятти

Эволюционная интеграция информационных технологий, направленных на хранение и обработку огромных массивов разнородной и слабоструктурированной информации и информационно-телекоммуникационных технологий, направленных на создание телекоммуникационных сетей, в соответствии с теорией больших систем привела, за счет так называемого системного эффекта эмерджентности к формированию новой структуры, обладающей новыми свойствами, которыми не обладает ни один элемент в отдельности, а именно информационного виртуального пространства, в котором информация существует в особой, в частности для традиционного права, электронной форме. Эффект эмерджментности и большое количество пользователей в силу синергического эффекта привело к формированию глобального межгосударственного цифрового пространства, позволившего обеспечить доступ к огромным информационным ресурсам большинству жителей Земли. В свою очередь стремительное развитие мирового цифровое пространство явилось аттрактором перехода к следующей стадии в развитии человеческого общества - информационному обществу.

Большинство ученых XX - XXI в.в., как в области гуманитарных, в том числе юриспруденции, наук так и естественно - технических наук связывали развитие цивилизации на основе перехода к информационному обществу, в основе которого лежат информация и знания, а соответственно в которой решающую роль будут играть отрасли, связанные с их получением, распространением и обработкой

Сущность информационного общества составляют следующие взаимосвязанные процессы:

— опережающий рост рынка информации и знания как фактора производства, по сравнению с рынками природных ресурсов, труда и капитала;

— высокий уровень информационных потребностей всех членов общества;

—информационная инфраструктура превращается в условие, определяющее не только национальную конкурентоспособность, но и национальную безопасность;

— информация и знания становятся движущей силой, определяющей политику, экономику, социальную жизнь.

Однако переход к информационному обществу характеризуется рядом противоречий. Одним из центральных является то, что темпы развития информационного общества таковы, что право отстает от его потребностей и потому многие общественные отношения, уже де факто действующие в информационной сфере, например, Интернете остаются де юре неурегулированными.

Кроме этого, анализ законотворческих процессов показывает, что в своей реализации они все больше приближаются к виду специальных информационных технологий, например то же административное право, уже просто немыслимо без компьютерных технологий ведения соответствующих документальных массивов (баз и банков данных).

Одним из основополагающих принципов информационного обеспечения для сферы государственного управления становится требование "информационной прозрачности" административной системы.

Указанные выше и другие динамично нарастающие потребности информационного общества в правовом регулировании возникающих в нем информационных общественных отношений предопределяет интерес ученых - юристов и специалистов-практиков к роли информации в обществе и связанных с ней информационно-правовым отношениям, что позволяет говорить о формировании новой отрасли права - информационного права [2].

Таким образом, формирование информационного права является следствием формирования информационного общества.

Существующая структура отрасли информационного права включает следующие подотрасли: компьютерное право, право информационной безопасности, право массовой информации, интернет-право, регулирующие определенные виды информационных отношений, являющихся особым родом общественных отношений.

Информационная безопасность является многогранным понятием, об этом свидетельствует существующее множество его определений. Поэтому целесообразно рассмотреть основные подходы к формированию этого понятия.

В рамках одного подхода под информационной безопасностью понимают - состояние общества, при котором обеспечена защита личности, общества и государства в информационном пространстве от воздействия на них организованных или стихийно возникающих информационных потоков.

В рамках другого подхода содержание информационной безопасности сводиться к трем ключевым составляющим:

1) состояние безопасности информационного пространства;

2) состояние безопасности информационной инфраструктуры;

3) состояние безопасности самой информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность, доступность.

Третий подход исходит из того, что информационное пространство представляет собой симбиоз информационно-технической (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологической составляющих. Следовательно, информационную безопасность общества можно также представить как интеграцию информационно-технической и информационно-психологической безопасностей.

Анализ, рассмотренных выше подходов показывает, что информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение защиты информации, но и объектов и методов этой защиты.

Особое место отводится информационной безопасности в современных условиях в области гражданского права.

В соответствии с теорией гражданского права, объектами гражданских прав, для которых вопросы информационной безопасности наиболее значимыми являются [1]:

- Информация как объект гражданских прав;
- Интеллектуальная собственность как объект гражданских прав;
- Личные неимущественные права.

Информация является объектом гражданских прав только в том случае, если ее обладатель может извлечь какую-либо имущественную выгоду. Обычно эта информация определяется как служебная или коммерческая тайны.

Например, работники, разгласившие тайну вопреки трудовому договору, обязаны возместить причиненные убытки.

Гражданско-правовое регулирование вопросов интеллектуальной собственности особенно актуально, в силу простоты технической реализации и быстродействия операций копирования и распространения, при использовании программного обеспечения.

Особую группу объектов гражданских прав, для которых гражданско-правовое регулирование сегодня социально значимо, образуют личные неимущественные права, под которыми понимаются не отделимые от личности их носителя блага и свободы, такие как жизнь, здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная, медицинская, банковская тайна и т.д.

Это связано с тем, что при правовом регулировании взаимоотношений в Интернете необходимо учитывать:

1. Такие предметы отношений, как сайт, веб-страница, домен, IP-адрес, электронно-цифровая подпись, электронная почта, аккаунты в социальных сетях и т.п.
2. Анонимность пользователей.
3. Низкая стоимость доступа к сети Интернет.
4. Высокая скорость распространения информации.
5. Простота охвата большой аудитории.

С учетом данных обстоятельств проблема обеспечения информационной безопасности в контексте развития норм гражданского права представляется весьма актуальной как в научном, так и в прикладном плане.

Библиографический список

1. Кашанина, Т.В., Кашанин, А.В. Основы российского права: К31 Учебник для вузов. — 3-е изд., перераб. и доп. — М.: Издательство НОРМА, 2003. — 784 с.

2. Ковалева, Н.Н. Информационное право России (2-е издание): учебное пособие / Ковалева Н.Н. М.: Дашков и К, Ай Пи Эр Медиа, 2016. — 352 с.

3. Ловцов, Д.А. Система принципов эффективного правового регулирования информационных отношений в инфосфере / Д.А. Ловцов//Информационное право. – 2017. - №1. - С. 13-18.

4. Лопатин, В.Н. Риски информационной безопасности при переходе к цифровой экономике/В.Н. Лопатин//Государство и право. – 2018. - №3. - С. 77-89.

ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ"

*Николаев А.Н.**, студент*
Научный руководитель: Горбачевская Е.Н., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и

о защите информации" от 27 июля 2006 года номер 149-ФЗ (принят Государственной Думой 8 июля 2006 года). В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при:

– осуществлении права на поиск, получение, передачу, производство и распространение информации;
– применении информационных технологий;
– обеспечении защиты информации.

Процитируем основные определения:

Информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации - возможность получения информации и ее использования;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Мы, разумеется, не будем обсуждать качество данных в Законе определений. Обратим лишь внимание на нетрадиционность определения конфиденциальности информации, приравнивающего конфиденциальность к неразглашению.

В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

установление ограничений доступа к информации только федеральными законами;

открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

обеспечение безопасности Российской Федерации при создании информационных си-

стем, их эксплуатации и защите содержащейся в них информации;

достоверность информации и своевременность ее предоставления;

неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Отметим, что в этих принципах явным образом фигурируют целостность (достоверность) и доступность (своевременность предоставления) информации.

В статье 9 Закона содержатся следующие положения:

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Отметим, что в этой статье упор делается на конфиденциальность информации.

Статья 11 "Документирование информации" содержит следующие важные положения:

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Статья 16 целиком посвящена вопросам защиты информации. Процитируем ее полностью.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

– предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

В процитированной статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации.

Явным образом не упомянуты такие меры, как аккредитация, сертификация и лицензирование, но в пунктах 5 и 6 они, конечно, подразумеваются.

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информационных технологиях и о защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

Библиографический список

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: РиС, 2014. - 586 с.

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

3. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с.

4. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. - 392 с.

5. Ищейнов, В.Я. Защита конфиденциальной информации: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. - 256 с.

6. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.

7. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.

8. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. - М.: ДМК Пресс, 2012. - 592 с.

9. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 592 с.

10. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Плотников А.П., студент
Научный руководитель: Горбачевская Е.Н., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Характерной особенностью современного общества является информатизация практически всех сфер его жизнедеятельности. При этом количество информации потребляемой обществом стремительно увеличивается с каждым годом. В качестве средств современное информационное общество широко использует компьютерные технологии, телекоммуникационные сети, электронные библиотеки, банки данных, автоматизированные системы, системы искусственного интеллекта. При этом главной проблемой, возникающей перед обществом, становится проблема обеспечения информационной безопасности. По данным аналитиков за последние годы злоумышленные действия над информацией не только не уменьшаются, а имеют достаточно устойчивую тенденцию к росту.

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; даже проводится ФЗ о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности Российской Федерации хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Использование надежного пароля является одним из наиболее важных факторов защиты компьютера от злоумышленников и других нежелательных пользователей.

Пароль — это условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.

В 2003году Infosecurity провели небольшое исследование, с целью выявления самых популярных паролей. Было опрошено 152участника и в итоге были получены следующие результаты[3]:

– ·16% использовали собственное имя;
– ·12% использовали слово“password”;
– ·11% использовали название любимой спортивной команды;
– ·8% использовали дату рождения.

В начале 2013года, в Лаборатории Касперского провели свое исследование с тем же вопросом, но уже в 25странах. Картинка немного изменилась[3]:

– ·16% использовали собственную дату рождения;
– ·15% использовали сочетание цифр «123456»;
– ·6% использовали слово “password” на местном языке;
– ·6% использовали кличку домашнего животного.

Использование представленных паролей не может служить эффективной защитой ин-

формации. Пароль, несущий в себе высокую степень защиты, должен отвечать следующим требованиям:

- ·длина не менее 6—8символов;
- ·использование цифр;
- ·использование букв разных регистров;
- ·использование букв разных алфавитов;
- ·использование специальных символов;
- ·отсутствие словарных выражений.

Использование паролей в организации также должно регламентироваться административными методами:

Необходимо выделять программы и объекты информации, которые подлежать защите данным способом;

Доступ к паролю к каждому ресурсу должен быть ограничен узким кругом ответственных лиц, как правило, исполнителем, пользующимся защищенным ресурсов, руководителем подразделения или системным администратором;

Также должны быть разработаны правила хранения паролей, их смена в случаях взлома, утери и т.д.

Библиографический список

1. Компания «СёрчИнформ» [Электронный ресурс] — Режим доступа: URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

2. «Научный форум». Проект издательства «Международный центр науки и образования» [Электронный ресурс] — Режим доступа: URL: https://nauchforum.ru/studconf/tech/xix/5604

3. Центр научного сотрудничества «Интерактивплюс» [Электронный ресурс] — Режим доступа: URL: https://interactive-plus.ru/ru/article/463753/discussion_platform

ВИДЫ РЕЗЕРВНОГО КОПИРОВАНИЯ, ИХ ПЛЮСЫ И МИНУСЫ

Пономарев Д.В., студент
Научный руководитель: Куралесова Н.О., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Резервное копирование – это затратный, но необходимый процесс, страхующий своих владельцев от безвозвратной потери данных. Он полезен как для отдельных пользователей, так и для целых фирм. Благодаря резервному копированию можно легко восстановить большой объем данных, потерянных вследствие воздействия вируса, ошибки или же физического повреждения.

Под резервное копирование обычно выделяются отдельные сервера, которые, в идеале, должны находиться отдельно от основных, это даст дополнительную защиту для хранимой информации, например от потопа или пожара.

Резервное копирование бывает следующих видов:

Полное резервное копирование (Fullbackup, полный бэкап)

Полное копирование обычно затрагивает всю вашу систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно оно выполняется по пятницам или в течение выходных, когда копирование большого объёма данных не влияет на работу организации. Последующие резервные копирования, выполняемые с понедельника по четверг до следующего полного копирования, могут быть дифференциальными или инкрементными, главным образом для того, чтобы сохранить время и место на носителе. Полное резервное копирование следует прово-

дить, по крайней мере, еженедельно.

На рисунке 1 все бэкапы — полные.

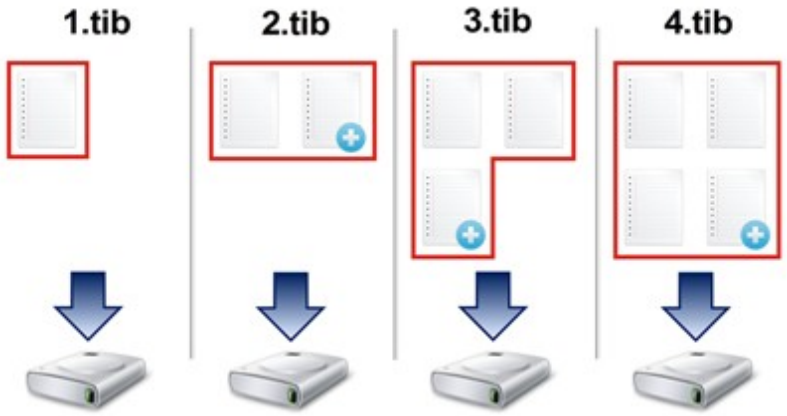


Рисунок 1 - Бэкапы — полные

Такие бэкапы самые надежные, но и самые большие. При этом для восстановления потребуется только один файл.

Плюсы: Гарантирует целостность и точность сохраненной информации, погрешности исключаются.

Минусы: Полное копирование трудоемкий процесс и затратный на время, во время его проведения проблематичная работа с системой (она занята копированием). Восстанавливаются файлы в том виде, в каком были во время последнего резервного копирования, всё что было позднее - пропадает.

Дифференциальное резервное копирование (Differentialbackup, дифференциальный бэкап)

При разностном (дифференциальном) резервном копировании каждый файл, который был изменен с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все, что вам необходимо - это последняя полная и последняя дифференциальная резервная копия. Популярность дифференциального резервного копирования растет, так как все копии файлов делаются в определенные моменты времени, что, например, очень важно при заражении вирусами.

На рисунке 2 1.tib — полное резервирование (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — дифференциальные бэкапы.

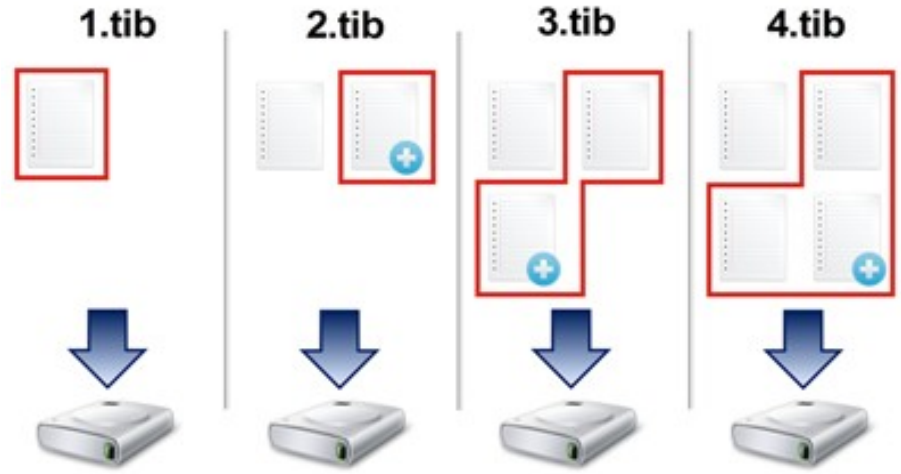


Рисунок 2 - 1.tib — Полное резервирование (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — дифференциальные бэкапы

У всех последующих бэкапов общая часть состоит в полном бэкапе. Т.е. каждый после-

дующий дифференциальный бэкап это продолжение и дополнение первого. Для восстановления потребуется сам дифференциальный бэкап и предыдущий полный бэкап (на рисунке — 1.tib).

Плюсы: Меньше по объему, чем полные, и больше, чем инкрементные. Представляют собой середину.

Минусы: Со временем накапливаются и в итоге могут быть больше чем, полный бэкап.

Инкрементное резервное копирование (Incrementalbackup, инкрементный бэкап)

При добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее инкрементное резервное копирование добавляет только файлы, которые были изменены с момента предыдущего. В среднем, инкрементное резервное копирование занимает меньше времени, так как копируется меньшее количество файлов. Однако процесс восстановления данных занимает больше времени, так как должны быть восстановлены данные последнего полного резервного копирования, плюс данные всех последующих инкрементных резервных копирований. При этом в отличие от дифференциального копирования изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо.

На рисунке 3 1.tib — полный бэкап (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — инкрементные бэкапы.

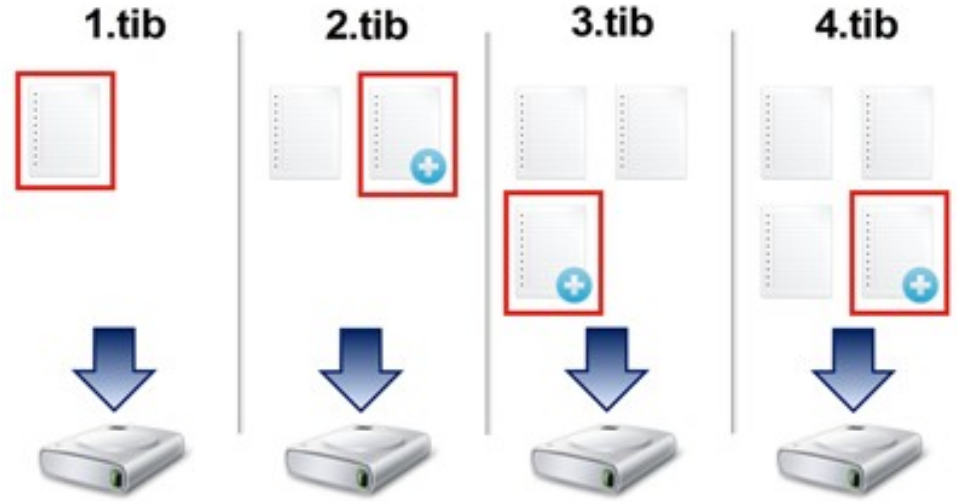


Рисунок 3 - 1.tib — полный бэкап (первый бэкап всегда полный), 2.tib, 3.tib, 4.tib — инкрементные бэкапы

Для восстановления потребуется предыдущий полный бэкап (на рисунке 3— 1.tib) и вся цепочка инкрементных бэкапов заканчивая тем бэкапом, из которого вы хотите восстановить данные.

Плюсы: Инкрементные бэкапы гораздо меньше полных.

Минусы: Для восстановления требуется вся цепочка сохранений. При повреждении одного из «звеньев» последующее восстановление невозможно.

Три метода резервного копирования дают нам массу всевозможных вариантов, так называемых цепочек бэкапов. Цепочка – это один полный бэкап и все зависящие от него инкрементные и/или дифференциальные бэкапы.

Но это виды резервирования, предназначенные для больших массивов данных, и для их использования созданы всевозможные программы, существуют и другие виды копирования и сохранения данных.

Клонирование

Клонирование позволяет копировать целые разделы или носитель (устройство) со всеми файлами в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным.

Резервное копирование в виде образа

Образ — точная копия всего раздела или носителя (устройства), хранящаяся в одном файле. Иными словами архивирование и хранение в таком виде с возможностью дальнейшего извлечения. Исключает возможность редактирования.

Есть три способа копирования данных:

Резервное копирование в режиме реального времени

Резервное копирование в режиме реального времени позволяет создавать копии файлов, директорий и томов, не прерывая работу, без перезагрузки компьютера.

Холодное резервирование

При холодном резервировании база данных выключена или закрыта для потребителей. Файлы данных не изменяются и копия базы данных находится в согласованном состоянии при последующем включении.

Горячее резервирование

При горячем резервировании база данных включена и открыта для потребителей. Копия базы данных приводится в согласованное состояние путём автоматического приложения к ней журналов резервирования по окончании копирования файлов данных.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ (НА ПРИМЕРЕ ЭКСПЛУАТАЦИИ И ВНЕДРЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПАНИИ 1С)

Пырков П.В., студент
Научный руководитель: Федосеева О.Ю., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

«**Информационная безопасность** - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная, или например, физическая). Основная задача информационной безопасности - сбалансированная защита конфиденциальности, целостности и доступности данных. Ключевые принципы: **Конфиденциальность, Целостность, Доступность, Невозможность отказа»** [1].

Рассмотрим принципы, характеризующие информационную безопасность на примере эксплуатации и внедрения программного обеспечения (далее ПО) компании 1С на предприятии.

Конфиденциальность

«**Конфиденциальность** информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомлённости. Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей. Шифрование информации — характерный пример одного из средств обеспечения конфиденциальности».

При развертывании ПО 1С на предприятии для хранения данных используются популярные базы данных (MS SQL, Postgresql,DB2), которые в свою очередь уже обеспечиваю высокий уровень информационной безопасности. Следующим этапом управляемого доступа к данным, является авторизация пользователя в данной системе. Главными идентификаторами пользователя являются его уникальный логин (англ. login - имя (идентификатор) и его пароль. Основная проблема в современных информационных системах, это не достаточная сложность пароля, которая даём злоумышленникам возможность его подбора. Причиной всех случаев взлома информационных систем до 80% называется низкая сложность паролей. Высокая сложность пароля достигается разными способами от длины пароля и до использования специальных символов и их чередования. Данная проблема характерна не только для

ПО, но и также любых устройств (телефоны, wi-fi роутеров и др.) к которым осуществляется доступ. Дальнейшее обеспечение конфиденциальности достигается разграничением доступа к данным в самой информационной системе между пользователями на основании присвоенным им ролям. За это отвечает хорошо развитая в 1С система RLS (**Record Level Security - ограничение прав на уровне записи**). Продуманная система RLS обеспечит высокий уровень защиты данных. Далее рассмотрим следующий принцип.

Целостность

Чёткое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки.

Как было сказано выше использование в решениях 1С баз данных, обеспечивает не только конфиденциальность, но и сохранность этих данных. Главным образом это достигается непрерывным резервным копированием баз данных, а также хранением этих данным на разных серверах предприятия с использование отказоустойчивых систем на основе кластеров.

Однако её целостности угрожают компьютерные вирусы и логические бомбы, ошибки программирования и вредоносные изменения программного кода, подмена данных, бэкдоры (уязвимости в программном обеспечении) и тому подобное. Рассмотрим более подробно эти угрозы.

Основным источников угроз в наше время является интернет. Для предотвращения этих угроз используются как программные средства, так и аппаратные решения.

Программно-технические способы и средства обеспечения информационной безопасности.

В литературе предлагается следующая классификация средств защиты информации:

– Средства защиты от несанкционированного доступа
  – Средства авторизации;
  – Мандатное управление доступом;
  – Избирательное управление доступом;
  – Управление доступом на основе ролей;
  – Журналирование (так же называется Аудит).
– Системы анализа и моделирования информационных потоков (CASE-системы).
– Системы мониторинга сетей:
  – Системы обнаружения и предотвращения вторжений (IDS/IPS).
  – Системы предотвращения утечек конфиденциальной информации (DLP-системы).
– Анализаторы протоколов.
– Антивирусные средства.
– Межсетевые экраны.
– Криптографические средства:
  – Шифрование;
  – Цифровая подпись.
– Системы резервного копирования.
– Системы бесперебойного питания:
  – Источники бесперебойного питания;
  – Резервирование нагрузки;
  – Генераторы напряжения.
– Системы аутентификации:
  – Пароль;

– Ключ доступа (физический или электронный);
– Сертификат;
– Биометрия.
–Средства предотвращения взлома корпусов и краж оборудования.
–Средства контроля доступа в помещения.
–Инструментальные средства анализа систем защиты:
–Антивирус.

Для защиты целостности информации необходимо применение множества разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Для обеспечения контроля целостности ПО компания 1С для разработчиков предоставляет хранилище конфигурации, где хранится вся история изменений программного кода. Компания 1С постоянно выпускает обновления для своих прикладных решений, что позволяет поддерживать ПО в актуальном состоянии.

Доступность

Согласно этому принципу, информация должна быть доступна авторизованным лицам, когда это необходимо. Основными факторами, влияющими на доступность информационных систем, являются DoS-атаки (аббревиатура от *Denial of Service* с англ. — «отказ в обслуживании»), атаки программ-вымогателей. Для обеспечения этого принципа в первую очередь необходимо использовать резервные каналы связи, а так же кластеры баз данных и кластеры серверов 1С расположенных в разных местах. В последнее время есть большое количество как аппаратных, так аппаратно-программных решений противодействия атакам из интернета в первую очередь DoS-атакам. Многие провайдеры провайдеры предоставляют свои услуги в этом направлении.

Невозможность отказа

Термин «невозможность отказа» (англ. *Non-Repudiation*, иногда употребляется слитно - *Nonrepudiation*) впервые появился в 1988 году в международном стандарте «Безопасность взаимосвязи открытых систем» (ISO 7498-2). Обычно понимается, как противоположный по смыслу термину англо-саксонского права *Repudiation* с англ. — «отказ, отрицание», имеющего два основных толкования. С одной стороны, он означает фундаментальное право стороны отказаться от исполнения обязательств по сделке на законных основаниях, если, например, подпись на бумажном документе была подделана, либо оригинальная подпись была получена незаконным путём (в результате мошенничества). При этом бремя доказательства подлинности подписи лежит на той стороне, которая на неё полагается. Другая интерпретация - неправомерный отказ от обязательств. В контексте компьютерной безопасности это может быть, например, отрицание одной из сторон факта отправки, приёма, авторства, либо содержания электронного сообщения. В контексте информационной безопасности «невозможность отказа» понимается как подтверждение целостности и оригинального происхождения данных, исключающее возможность подделки, которое может быть в любой момент проверено сторонними лицами, либо как установление идентичности (личности, документа, объекта), которое с высокой степенью достоверности может считаться подлинным, и не может быть опровергнуто.

Компания 1С в основные конфигурации, как-либо связанные с документооборотом, включает данный функционал. Использование электронных подписей документов, используемый в нашей стране разными организациями и структурами, позволяет реализовать данный принцип информационной безопасности в решениях от компании 1С.

Библиографический список

1. Информационная безопасность. Wikipedia. [Электронный ресурс] — Режим доступа: https://ru.wikipedia.org/wiki.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ТЕХНОЛОГИЧЕСКОМ ОБОРУДОВАНИИ

Ремнева О.Ю., к. т. н.
Волжский университет имени В.Н. Татищева
г. Тольятти

Процесс всеобщей автоматизации производственного процесса не мог не затронуть и такой его аспект, как упаковка и транспортировка продукции от стадии «заготовка» до стадии «готовое изделие». В частности особый интерес вызывает упаковка и, как следствие, сохранение товарного вида и рабочих характеристик крупногабаритных изделий.

Существуют различные способы упаковки габаритных изделий [1, 2, 3, 4 и др.], каждый из которых представляет практический интерес в условиях того или иного производства.

Рассмотрим оборудование для обертывания габаритных изделий и упаковке габаритных изделий, получаемой таким образом. Данное оборудование может быть использовано в машиностроении, строительстве, а так же при производстве мебели.

Процесс обертывания и/или упаковки осуществляется за счет одновременного вращения оберточного блока вокруг поступательно перемещающегося вдоль траектории обертывания изделия. При этом происходит автоматическое обертывание оберточного материала на всю длину изделия.

Данное технологическое оборудование работает в непрерывном режиме, с задаваемым усилием намотки. В связи с чем, особую роль в обеспечении безопасности работы оператора на данном оборудовании является наличие автоматической системы отключения при попадании в зону намотки любого элемента с параметрами, отличными от заданных [5].

С задачей определения присутствия детали на конвейере автоматизированной линии, а так же получения информации о структуре и составе продукции помогают справиться датчики. Есть множество типов датчиков: магнитные, индуктивные, фотоэлектрические, емкостные - каждый из них имеет свои достоинства и недостатки.

Оптические бесконтактные выключатели (датчики) широко применяются сегодня во многих отраслях, где используется оборудование, предназначенное для позиционирования, счета, да и просто для обнаружения различных объектов. Применение кодирования в схемах датчиков позволяет избежать постороннего влияния на них источников света, и защищает, таким образом, от ложных срабатываний. Для функционирования в условиях низких температур предназначены датчики в термокожухах.

Данные приборы представляют собой электронные схемы, реагирующие на изменение светового потока, падающего на приемник, благодаря которому фиксируется наличие или отсутствие объекта в определенной области пространства. Кодирование светового излучения источника (пространственная селекция и модуляция) повышает эффективность, и, как упоминалось выше, сводит на нет влияние помех [5].

Конструктивно система датчика включает в себя два главных функциональных блока — источник излучения и его приемник (рисунок 1). Это могут быть два отдельных корпуса, либо один корпус для обоих блоков, в зависимости от принципа работы конкретного датчика (выключателя).

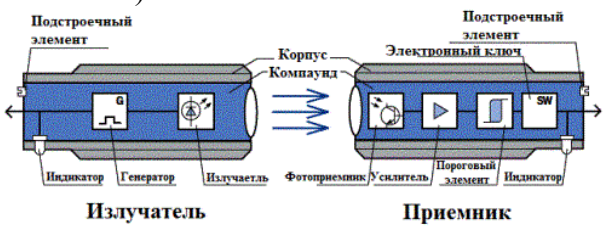


Рисунок 1 – Конструкция оптического бесконтактного датчика

По принципу работы оптические датчики бывают трех типов: Барьерный (тип T) (рисунок 2), Диффузный (тип D) (рисунок 3) и Рефлекторный (Тип R) (рисунок 4).

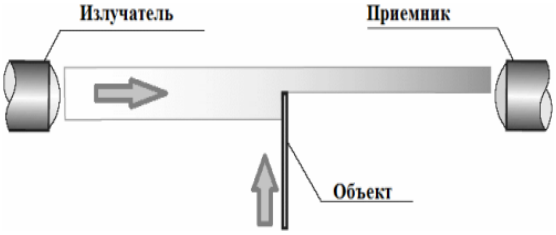


Рисунок 2 – Оптический датчик барьерного типа

Оптические выключатели барьерного типа работают на прямом луче, и содержат две отдельные части, передатчик и приемник, которые должны быть расположены соосно друг напротив друга, чтобы поток излучения, испускаемый излучателем (передатчиком) был направлен и точно попадал на приемник [5].

Когда луч прерывается объектом, происходит срабатывание выключателя. Датчики данного типа могут работать при расстоянии в десятки метров между передатчиком и приемником, к тому же они обладают хорошей помехозащищенностью, им не страшны ни пыль, ни капли жидкости и т. д.

Но есть и недостатки:

– прокладывать провода питания отдельно к каждой из двух частей приходится иногда на большие расстояния;

– хорошо отражающие предметы могут вызвать ложные срабатывания;

– прозрачные предметы могут не достаточно ослабить луч, требуется это учитывать.

Для приемлемого устранения названных недостатков и служит регулятор чувствительности. И, конечно, минимальный размер обнаруживаемого объекта не должен быть меньше диаметра луча.

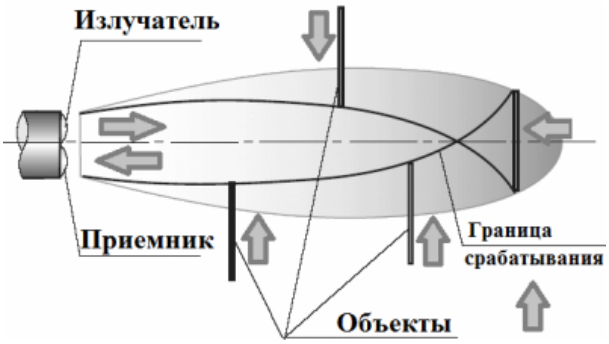


Рисунок 3 – Оптический датчик диффузного типа

Датчики диффузного типа используют отраженный от объекта луч, зеркальное отражение. Приемник и передатчик находятся в едином корпусе. Излучатель направляет поток на объект, луч отражается от его поверхности в разных направлениях, в зависимости от оптических особенностей объекта. Частично поток возвращается назад, где улавливается приемником, и происходит срабатывание выключателя.

Важно здесь учесть то, что ложные срабатывания могут быть вызваны отражающими объектами, расположенными за рабочей областью установки, за контролируемым объектом. Для устранения таких помех применяют выключатели с функцией подавления фона (таблица 1) [5].

Таблица 1 – Таблица поправочных коэффициентов

Таблица поправочных коэффициентов	K
Белая бумага	1,20
Картон	0,80
Древесина чистая	1,20
Черная резина	0,03
Непрозрачный черный пластик	0,20
Непрозрачный белый пластик	1,50
Прозрачная пластиковая бутылка	0,60
Прозрачная корич. пластиковая бутылка	1,00
Алюминий необработанный	2,50
Алюминий обработанный	1,70
Сталь нержавеющая	7,50
Горячекатаная сталь	1,00
Холоднокатаная сталь	1,50

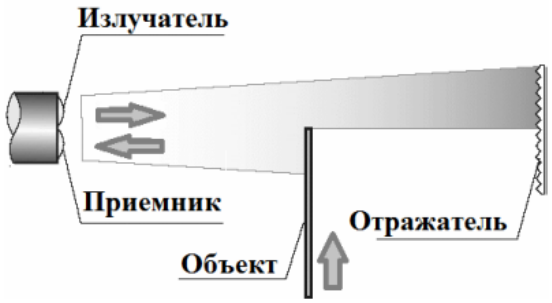


Рисунок 4 – Оптический датчик рефлекторного типа

Здесь используется отраженный от рефлектора луч. Приемник с излучателем в одном корпусе, луч, падая на рефлектор, отражается, попадает на приемник, происходит срабатывание. Когда объект выходит из рабочей зоны, происходит еще одно срабатывание [5].

Таким образом, для обеспечения безопасности работы оператора на рассматриваемом оборудовании, в монтируемой системе автоматического отключения целесообразно применение оптических датчиков рефлекторного либо диффузного типа.

Библиографический список

1. Заявка 2233779 Российская Федерация, МПК B65B 19/22 (2000.01). Способ и машина для обертывания изделия [Текст] / Гини М. (Италия), Спатафора М. (Италия); заявитель Г.Д Сочиета пер ациони; пат. поверенный Томская Е.В. – № 99114777/12; заявл. 07.07.99; опубл. 10.08.04, Бюл. № 22; приоритет 08.07.98, BO98A 000417 (Италия).

2. Пат. 2404893 Российская Федерация, МПК B29C65/74 (2006.01). Устройство для обертывания разнообразных изделий / Фарнети А. (Италия). Бюл. 33, 2010.

3. Заявка 2010147647 Российская федерация, МПК B65B 11/42 (2006.01). Способ и машина для формирования запечатанной обертки вокруг изделия и упаковка, образованная таким образом [Текст] / Чиволани Д. (Италия), Каррара М. (Италия); заявитель Ационария конструкциони маккине аутоматике А.К.М.А. С.П.А. (Италия) . – № 2010147647/13; заявл. 21.04.09; опубл. 27.05.12; приоритет 23.04.08, BO2008A000254 (Италия).

4. Пат. 155472 РФ, МПК B65B 33/00 (2006.01). Станок для упаковки изделий в растягивающуюся полимерную пленку, преимущественно для упаковки оконных и/или дверных конструкций / Чернопрудов С. Г. Бюл. № 28, 2015.

5. Школа для электрика [Электронный ресурс].- Режим доступа: http://electricalschool.info/spravochnik/apparaty/1726-opticheskie-beskontaktnye-vykljuchateli.html, свободный. – Загл. с экрана.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ, ИХ ПРЕИМУЩЕСТВА

Федосеев М.Ю., студент
Самарский национальный исследовательский университет имени академика С.П. Королева
г. Самара

В настоящее время уже сложно представить себе ИТ-отрасль без виртуализации, развитие информационных систем организаций тесно связано с применением технологий виртуализации. Причем данные технологии позволяют значительно сократить расходы, связанные с приобретением и обслуживанием серверных систем, сократить время на восстановление информации или развертывания аналогичных систем в новом оборудовании.

В настоящее время все большую популярность набирают технологии виртуализации. И это не случайно – вычислительные мощности компьютеров растут. В результате развития технологий, появляются шести-, восьми-, шестнадцатиядерные процессоры (и это еще не предел). Растет пропускная способность интерфейсов компьютеров, а также емкость и отзывчивость систем хранения данных. В результате возникает такая ситуация, что имея такие мощности на одном физическом сервере, можно перенести в виртуальную среду все серверы, функционирующие в организации (на предприятии). Это возможно сделать с помощью современной технологии виртуализации.

Технологии виртуализации в настоящее время становятся одним из ключевых компонентов современной ИТ-инфраструктуры крупных предприятий (организаций). Сейчас уже сложно представить построение нового серверного узла компании без использования технологии виртуализации. Определяющими факторами такой популярности, несмотря на некоторые недостатки, можно назвать экономию денег и времени, а также высокий уровень безопасности и обеспечение непрерывности бизнес-процессов.

Защита виртуальных сред информации в виртуальных инфраструктурах сегодня актуальна как никогда.

Технология виртуализации подразумевает наличие дополнительного компонента — гипервизора, который не исполняет стороннего кода и контролирует работу приложений во всех виртуальных средах. Проверка на потенциальную опасность, организованная через гипервизор, работает более надежно, поскольку вредоносный код не может ей противостоять. Атаки же на сам гипервизор затруднены тем, что он не исполняет пользовательского кода и все драйвера поставляются разработчиком платформы виртуализации. При этом безопасность гипервизора тем выше, чем он компактнее. Гипервизор же VMware «на порядок компактнее конкурирующих», поэтому атаковать его еще сложнее, чем Hyper-V или Xen, работающие внутри базовой операционной системы, где в принципе можно запускать сторонние приложения. Таким образом, виртуализация служит дополнительным уровнем защиты при попытке захвата приложений или данных пользователей.

Кроме того, платформу виртуализации можно использовать для решения определенных задач информационной безопасности. В частности, в виртуальной среде можно проводить тестирование обновлений программ, чтобы проверить устойчивость их работы в «боевой» системе. Также в виртуальных средах можно легко развернуть серверы-ловушки для хакеров, которые внешне выглядят очень привлекательно для взлома, но реальных данных не содержат. Контролируя такую ловушку через гипервизор, администратор может выявить целенаправленные атаки и собрать сведения для поимки преступников. Расследование инцидентов в виртуальной среде также упрощается, поскольку взломщику сложнее добраться до системных журналов и их «подчистить». К тому же образы виртуальных систем целиком могут быть сохранены в резервной копии для последующего пристального анализа экспертами-криминалистами. Все это дает основания представителям VMware утверждать, что виртуальная среда может быть защищена лучше, чем информационная система, не использующая виртуализацию.

Следует отметить, что технология виртуализации объединяет приложения и данные в единую среду. Если до недавнего времени данные и приложения защищались по различным сценариям: данные — при помощи систем резервного копирования, программы — установкой антивирусных средств, то с переходом на виртуализацию методы защиты программ и данных должны сблизиться. Появились технологии поиска вирусов внутри выключенной виртуальной машины — в частности, такой механизм реализован в Trend Micro Deep Security. Кроме того, с вредоносными программами начали бороться при помощи восстановления виртуальной среды из чистой и проверенной резервной копии. И этот процесс объединения методов защиты приложений и данных будет по мере распространения технологий виртуализации только расширяться.

Впрочем, чтобы виртуальные среды были безопаснее физических, нужно пользоваться предоставляемыми технологией виртуализации преимуществами. Недостаточно просто перенести уже построенную для физической инфраструктуры систему защиты на платформу виртуализации, нужно активно внедрять описанный выше дополнительный функционал: осуществлять контроль вирусов, поступающих извне виртуальной среды; устанавливать среды-ловушки; вести расследование инцидентов по резервным копиям виртуальных машин и др. Применяя эти современные методы защиты виртуальных приложений, предприятие будет иметь больше шансов сохранить контроль над своей информацией.

В соответствии с ГОСТ Р 56938-2016 Национальный стандарт РФ «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» (введен в действие 1 июня 2017 года) устанавливаются требования по защите информации, обрабатываемой с использованием технологий виртуализации, в нем рассматриваются угрозы безопасности и меры защиты информации, обрабатываемой с помощью технологий виртуализации.

Виртуализацией называют группу технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Под термином "виртуализация" объединяется множество информационных технологий, призванных снижать затраты на разворачивание компьютерной сети организации, повышать отказоустойчивость применяемых серверных решений, а также достигать других преимуществ. Виртуализация представляет собой имитацию программного и/или аппаратного обеспечения, в среде (на базе) которого функционируют различные программы.

Виртуализацию проводят в отношении:

- программ;
- вычислительных систем;
- систем хранения данных;
- вычислительных сетей;
- памяти;
- данных.

При использовании технологий виртуализации создаются (виртуальные и виртуализованные) объекты доступа, подлежащие защите наравне с другими объектами информационных систем, в том числе аппаратные средства информационных систем, используемые для реализации технологий виртуализации. К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);
- виртуальные вычислительные системы (ВМ, виртуальные сервера и др.);
- виртуальные системы хранения данных;
- виртуальные каналы передачи данных;
- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пас-

сивное сетевое оборудование и др.);

- виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;

- периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

Для защиты перечисленных объектов используют как виртуальные средства ЗИ и средства ЗИ, предназначенные для использования в среде виртуализации, являющиеся разновидностями средств ЗИ, так и другие виды средств ЗИ.

На протяжении последнего 10-летия сохраняется неизменно высокий интерес к технологии виртуализации, которая считается одной из наиболее перспективных среди доступных для компаний ИТ-технологий. VMWare, Microsoft, Intel и многие другие производители сегодня занимаются разработкой платформ виртуализации. Среди представленных на рынке одной из наиболее востребованных является платформа VMware. Использование этой технологии виртуализации позволяет не менее чем в два раза снизить расходы на программные и аппаратные ИТ-средства. Однако, как часто и бывает с новейшими разработками, защита информации пока осуществляется не на достаточном уровне. Причиной этого является то, что технологии VMware пришли на российский рынок недавно и находятся в процессе развития. Лидерами индустрии уже активно развивается защита виртуализации, но на сегодняшний день уровень безопасности все еще невысок. Согласно исследованию, проведенному агентством Gartner, 60% виртуальных машин защищены хуже, чем их физические аналоги. Одной из причин отсутствия надежной защиты виртуальных сред, как отмечает агентство, может быть тот факт, что 40% проектов виртуализации в компаниях запускаются без участия специалистов по информационной безопасности.

Преимущества технологии виртуализации. По мнению аналитической компании Gartner, технология виртуализации вошла в число 10 наиболее перспективных технологий для корпоративного сектора. Внедрение виртуализации позволяет снизить капитальные и эксплуатационные затраты на ИТ-инфраструктуру:

1. Сокращение затрат на приобретение и поддержку оборудования. В современных условиях практически в каждой компании всегда найдется один или два сервера имеющие несколько ролей, например, почтовый сервер, файловый сервер, сервер базы данных и т.д. Безусловно, на одной физической машине можно поднимать по несколько программных комплексов (серверов), выполняющих различные задачи. Но очень часто бывают ситуации, когда установка нового ПО требует независимой серверной единицы. В таком случае как раз и придет на выручку виртуальная машина с требуемой ОС. Сюда же можно отнести случаи, когда в сети необходимо иметь несколько независимых друг от друга виртуальных серверов со своим набором служб и своими характеристиками, которые должны существовать как независимые узлы сети. Типичный пример – это услуги VPS-хостинга. Экономия электроэнергии.

2. Сокращение серверного парка. Преимущество виртуализации состоит в том, что можно значительно сократить количество физических ЭВМ. В результате меньше времени и денег тратится на поиск, закупку и замену оборудования. Наряду с этим сокращаются площади, выделяемые под содержание серверной базы.

3. Сокращение штата IT-сотрудников. На обслуживание меньшего количества физических ЭВМ требуется меньше людей. С точки зрения руководства компании, сокращение штата — это сокращение серьезной статьи расходов предприятия.

4. Простота в обслуживании. Добавить жесткий диск или расширить существующий, увеличить количество оперативной памяти, все это занимает определенное время в случае с физическим сервером. Отключение, отсоединение из стойки, подключение нового оборудования, включение – в случае использования виртуализации все эти действия опускаются, и операция сводится к нескольким щелчкам мыши или командам администратора.

5. Клонирование и резервирование. Еще одним плюсом виртуализации является простота клонирования виртуальных машин. Например, компания открывает новый офис. При

этом серверная инфраструктура центрального офиса стандартизирована и представляет собой несколько серверов с одинаковыми настройками. Развертывание такой инфраструктуры сводится к простому копированию образов на сервер нового офиса, конфигурировании сетевого оборудования и изменению настроек в прикладном ПО.

Основные бизнес-применения виртуализации:

- Виртуализация серверов. Перенос физических серверов в виртуальные машины одного физического сервера, оснащенного средством виртуализации. Применяется для консолидации серверов, позволяет более эффективно управлять инфраструктурой, повысить надежность и снизить расходы (TCO). Примеры: VMware ESX Server + vCenter (vSphere), Microsoft Hyper-V + SCVMM, Citrix XenServer + Essentials.

- Виртуализация рабочих мест пользователей. Это централизованное хранение рабочих мест в виде виртуальных машин на сервере с последующей доставкой на физические рабочие места или предоставление удаленного доступа через виртуализацию представлений (терминальные сервисы). Применяется для сокращения расходов на администрирование и обновления ПО на рабочих местах, повышения безопасности информации на рабочих местах и сокращения расходов на лицензии ПО (в варианте терминальных сервисов). Примеры: VMware View, Microsoft MED-V, Citrix XenDesktop, Sun VDI.

К дополнительным возможностям виртуализации можно отнести:

– Локальные гипервизоры виртуальных машин (VMware Workstation и т.п.);

– Виртуализация приложений (VMware ThinApp, Microsoft App-V, Citrix XenApp).

Безопасность виртуальной инфраструктуры - композиции иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств. Использование технологий виртуализации создает предпосылки для появления угроз безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Защита среды виртуализации информационных систем компании требует эффективных решений для борьбы с новыми, ранее неизвестными угрозами. Среди угроз виртуализации, которым открыты данные технологии, можно отметить:

– угроза компрометации гипервизора (Hyper-V, vSphere) как нового, по сравнению с физической средой, элемента управления инфраструктурой;

– угроза утечки данных вследствие злонамеренных или непреднамеренных действий системного администратора, получающего доступ к данным и к инфраструктуре;

– клонирование\копирование, миграция, репликация, создание снимков виртуальных машин;

– компрометация консолидированного хранилища данных при консолидации нескольких серверов на одном аппаратном комплексе, если компания прибегает к серверной виртуализации;

– угроза несанкционированного доступа (НСД) администратора виртуальной инфраструктуры к настройкам и правам пользователей на сервере виртуализации;

– отсутствие контроля за всеми событиями информационной безопасности и невозможность расследования инцидентов при их возникновении.

Безопасность виртуальной инфраструктуры. Безопасность информации, обрабатываемой в виртуальной среде, - один из ключевых вопросов при внедрении технологии виртуализации:

– Виртуальным серверам присущи ровно те же уязвимости, что и физическим;

– Как и любая новая технология, виртуализация несет в себе новые угрозы безопасности.

Угрозы безопасности для виртуальных инфраструктур:

– Атака на гипервизор с виртуальной машины.

– Атака на гипервизор из физической сети.

– Атака на диск виртуальной машины.

– Атака на средства администрирования виртуальной инфраструктуры.
– Атака на виртуальную машину с другой виртуальной машины.
– Атака на сеть репликации виртуальных машин.
– Неконтролируемый рост числа виртуальных машин.
– Защита информации в соответствии с законодательством.

Одной из ключевых проблем использования технологий виртуализации является легитимность защиты информации, которая обрабатывается в виртуальной среде.

Согласно российскому законодательству организации обязаны обеспечить надлежащую защиту конфиденциальной информации, с которой они работают, в том числе с применением сертифицированных средств защиты.

Эти проблемы касаются как информации, содержащей сведения, составляющие государственную тайну, так и конфиденциальной информации – коммерческой тайны или персональных данных.

Недостатки традиционных средств защиты. Проблемы внедрения технологий виртуализации связаны с тем, что с одной стороны, традиционные средства защиты информации не всегда совместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. С другой стороны, они не защищают от новых угроз безопасности информации, специфичных для виртуальной инфраструктуры.

Если нарушитель получает доступ к среде виртуализации, операционная среда традиционных СЗИ оказывается полностью скомпрометированной.

Из среды гипервизора нарушитель может незаметно для традиционных СЗИ, работающих в виртуальных машинах:

– копировать и блокировать весь поток данных, идущий на все устройства (HDD, принтер, USB, сеть, дискеты);
– читать и изменять данные на дисках виртуальных машин, даже когда они выключены и не работают, без участия программного обеспечения этих виртуальных машин.

Библиографический список

1. ГОСТ Р 56938-2016 Национальный стандарт РФ «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».

2. Защита информации при использовании виртуализации. [Электронный ресурс] - Режим доступа: http://www.securitycode.ru/solutions/zashchita-informatsii-virtualization/.

3. Виртуализация. Википедия. [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/.

4. Виртуализация: новый подход к построению IT-инфраструктуры. [Электронный ресурс] - Режим доступа: http://www.ixbt.com/cm/virtualization.shtml.

5. Виртуализация. Классификация и области применения. [Электронный ресурс] - Режим доступа: http://www.tadviser.ru/index.php/.

6. Анализ современных технологий виртуализации. [Электронный ресурс] – Режим доступа: https://habr.com/company/southbridge/blog/212985/.

7. Защита виртуализацией. [Электронный ресурс] – Режим доступа: https://www.osp.ru/news/articles/2012/22/13015604/.

КЛАССИФИКАЦИЯ АНТИВИРУСНЫХ СИСТЕМ

Эркечев Р.О., студент
Научный руководитель: Третьякова Т.И., ст. преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Информационная безопасность (англ. *Information Security*, а также — англ. *InfoSec*) — практика предотвращения несанкционированного доступа, использования, раскрытия, иска-

жения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная, или например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации. Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

Классификация средств защиты информации в наше время - довольно обширная. Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации. В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, сторожа, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

3. Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

5. Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще, и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики - предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом (например, с помощью вакцинации). Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить раз-

множение и удалить компьютерные вирусы и другое вредоносное программное обеспечение. Наиболее эффективны в борьбе с компьютерными вирусами - антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

Сканеры

На рисунке 1 представлена экранная форма антивирусного сканера Dr.Web Cureit.

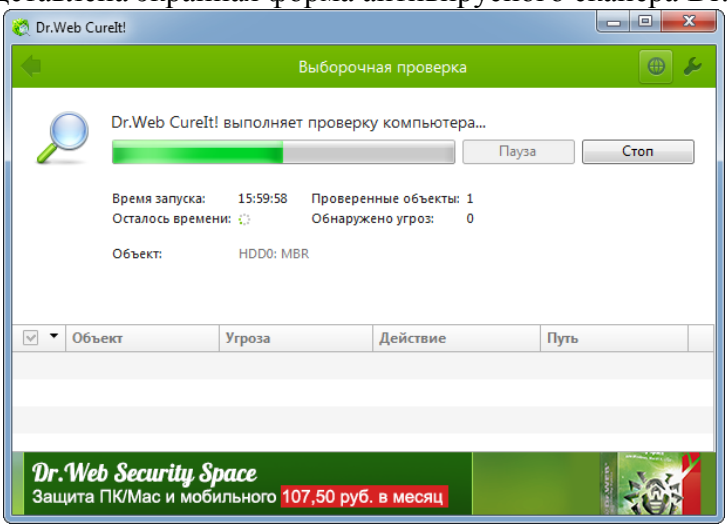


Рисунок 1 - Экранная форма антивирусного сканера Dr.Web Cureit

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые “маски”. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик - вирусов. Сканеры также можно разделить на две категории — “универсальные” и “специализированные”.

Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на “резидентные” (мониторы, сторожа), производящие сканирование “на-лету”, и “нерезидентные”, обеспечивающие проверку системы только по запросу. Как правило, “резидентные” сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как “нерезидентный” сканер способен опознать вирус только во время своего очередного запуска. С другой стороны резидентный сканер может несколько замедлить работу компьютера в том числе и из-за возможных ложных срабатываний.

Блокировщики

Антивирусные блокировщики — это резидентные программы, перехватывающие “вирусо-опасные” ситуации и сообщающие об этом пользователю. К “вирусо-опасным” отно-

сятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения. Иногда некоторые функции блокировщиков реализованы в резидентных сканерах. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно "выползает неизвестно откуда". К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (например, неизвестно ни об одном блокировщике для Windows95/NT — нет спроса, нет и предложения).

В течение семи лет, перепробованы разные антивирусные программы, начиная от «Avira», и заканчивая «ESET NOD 32». По моему мнению, в список лучших антивирусных программ входят:

1. Антивирус Касперского (Kaspersky Internet Security).
2. Eset NOD32 Internet Security.
3. Dr.Web.

Антивирус Касперского - антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»). Первоначально, в начале 1990-х, именовался **- V**, затем - **AntiViral Toolkit Pro**.

Кроме собственно антивируса также выпускается бесплатная лечащая утилита Kaspersky Virus Removal Tool.

ESET NOD32 - антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года. Название изначально расшифровывалось как «Nemocnica na Okraji Disku» («Больница на краю диска», перефраз названия популярного тогда в Чехословакии телесериала «Больница на окраине города»).

ESET NOD32 — это комплексное антивирусное решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, фишинг-атаки. В ESET NOD32 используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

Dr.Web - общее название семейства антивирусного ПО для различных платформ (Windows, macOS, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite). Разрабатывается компанией «Доктор Веб».

Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и превентивной защиты.

Не существует антивирусов, гарантирующих стопроцентную защиту от вирусов.

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаг, полифаг, программа-доктор) Применяются также различного типа блокировщики.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОСНОВНЫЕ ПОНЯТИЯ

Янюшев Э.Н., студент
Научный руководитель: Плюснина Е.В., ст. преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Введение. Широкое распространение вычислительной техники как средства обработки информации привело к информатизации общества и появлению принципиально новых, так называемых, информационных технологий.

Появление любых новых технологий, как правило, имеет как положительные, так и отрицательные стороны. Тому множество примеров. Атомные и химические технологи, решая проблемы энергетики и производства новых материалов, породили экологические проблемы. Интенсивное развитие транспорта обеспечило быструю и удобную доставку людей, сырья, материалов и товаров в нужных направлениях, но и материальный ущерб и человеческие жертвы при транспортных катастрофах возросли.

Информационные технологии, также не являются исключением из этого правила, и поэтому следует заранее позаботиться о безопасности при разработке и использовании таких технологий.

От степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

1. Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

2. Основные угрозы информационной безопасности

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- аппаратные средства - компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - дисководы, принтеры, контроллеры, кабели, линии связи и т.д.);
- программное обеспечение - приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- данные, хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- помехи в линиях связи из-за воздействий внешней среды.

3. Обеспечение информационной безопасности

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. законодательный (законы, нормативные акты, стандарты и т.п.);

2. морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);

3. административный (действия общего характера, предпринимаемые руководством организации);

4. физический (механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);

5. аппаратно-программный (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

4. Аппаратно-программные средства защиты информации

Несмотря на то, что современные ОС для персональных компьютеров, такие, как Windows 2000, Windows XP и Windows NT, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

4. 1. Системы идентификации и аутентификации пользователей

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы таких систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

4. 2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая криптографией (от греч. kryptos - скрытый и grapho – пишу).

4. 3.Системы шифрования данных, передаваемых по сетям

Различают два основных способа шифрования: канальное шифрование и оконечное (абонентское) шифрование.

В случае канального шифрования защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная информация остается открытой. Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

4. 4.Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

4. 5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Заключение. Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному

овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Многообразие условий, способствующих неправомерному овладению конфиденциальной информацией, вызывает необходимость использования не менее многообразных способов, сил и средств для обеспечения информационной безопасности,

Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременные меры предупреждения возможных угроз коммерческим секретам.

Обеспечение информационной безопасности достигается организационными, организационно-техническими и техническими мероприятиями, каждое из которых обеспечивается специфическими силами, средствами и мерами, обладающими соответствующими характеристиками.

ОАО «ФОСФОР» КАК УГРОЗА ЭКОЛОГИЧЕСКОЙ СИСТЕМЕ Г.О. ТОЛЬЯТТИ

Антонова М.С., студент
Научный руководитель: преподаватель Кузнецова К.А.
Тольяттинский социально-педагогический колледж
г. Тольятти

На сегодняшний день отходы являются основной экологической проблемой современного мира. Особо остро стоит вопрос об их утилизации.

С данной проблемой столкнулись жители г.о. Тольятти. Так, в промышленной зоне центрального района располагается заброшенный завод ОАО «Фосфор». Завод заброшен, а вместе с ним брошены производственные отходы. Общая площадь завода составляет 180 га, около 30 га из которых загрязнены фосфорсодержащими отходами. Имеющиеся на территории завода отходы несут реальную угрозу для здоровья жителей и окружающей их среды.

В настоящее время там находится около 7 тысяч тонн отходов I-IV классов опасности, в основном это фосфорсодержащий грунт, шлам, органические отходы, отходы жёлтого фосфора.

К примеру, желтый фосфор очень ядовитое огнеопасное вещество. В воде не растворяется, на воздухе легко окисляется и самовоспламеняется. При горении выделяет густой белый дым, который является очень токсичным. Так, в 2017 году было зарегистрировано 16 воспламенений желтого фосфора, а в 2016 году – 16.

Пары желтого фосфора вызывают:

- сильное раздражение глаз;
- слезотечение;
- раздражение дыхательных путей;
- глубокие, проникающие ожоги кожи.

Это говорит о том, что неутилизируемые отходы до сих пор являются опасными для здоровья. Отходы опасны, как и много лет назад, когда завод еще функционировал.

Работа завода завершилась в 2003 году, а попытки утилизировать отходы предпринимаются и по сегодняшний день. Данный вопрос многократно обсуждался как на городском, так и на областном уровне.

К примеру, в 2007 году из областного бюджета было выделено 5 миллионов рублей для обезвреживания наиболее опасных отходов. В ходе данной программы было утилизировано 60 тонн треххлористого фосфора и хлорокиси фосфора.

В 2011 году мэрия Тольятти приняла специальную долгосрочную программу по ликвидации экологического ущерба от прошлой деятельности предприятия. Но программа так и не была реализована.

В 2013 году ОАО "Фосфор" включили в федеральную целевую программу "Ликвидация накопленного экологического ущерба на 2014-2025 годы". Предполагалось, что на ликвидацию отходов государство выделит около 3 миллиардов рублей. Приступить к работам должны были в 2014 году, но работы так и не начались из-за отсутствия утвержденной программы.

В 2017 году попытки утилизировать отходы возобновились. Так, компания, по ликвидации отходов, выразила желание избавить город от опасных веществ 1 класса опасности за 7 миллионов рублей. Но попытка не увенчалась успехом, так как компания не имеет права на перевозку веществ 1 класса опасности. Также был шанс избавить город от желтого фосфора. Возможным его приобретателем мог быть Новоджамбульский фосфорный завод. Но специалисты, посетив наш город, и ознакомившись с товаром, отказались его приобретать. Причинной явилось то, что сырьё потеряло свои товарные свойства.

В 2018 году Министерство промышленности Самарской области обратилось с прось-

бой выделить 200 миллион рублей. Они необходимы для проведение инженерных изысканий с целью доказательства вреда, причиняемым фосфором окружающей среде. Это необходимо для того, чтобы включить фосфор в федеральный классификационный каталог отходов РФ. Только так фосфор можно будет утилизировать как отходы. И только тогда можно будет приступить к обезвреживанию территории. Стоимость реализации данного проекта 3 миллиарда рублей. Но для реализации одного из способов необходимо провести инвентаризацию отходов на территории ОАО «Фосфор», а также рассчитать стоимость утилизации.

Существуют способы для решения городской проблемы, но пока они не реализованы в жизнь. А это значит, что 7 тысяч тонн фосфоросодержащих отходов I-IV классов опасности, до сих пор являются угрозой для городской экосистемы.

Библиографический список

1. Васина, М.В. Разработка проекта нормативов образования отходов и лимитов на их размещение: учебное пособие [Текст] / М.В. Васина, Е.Г. Холкин. Издательство ОмГТУ, 2017. – 124 с.

2. Степанова, С.В. Процессы, аппараты и оборудование для защиты литосферы от промышленных и бытовых отходов: учебное пособие [Текст] / С.В. Степанова, С.М. Романова, А.Б. Ярошевский. – Издательство КНИТУ, 2012. – 144 с.

МОДЕРНИЗАЦИЯ ОЧИСТНЫХ СООРУЖЕНИЙ НИТРИДЕНИТРИФИКАЦИИ (НДФ) ЦЕХА 39 ПАО «КУЙБЫШЕВАЗОТ»

Денисова Н.С., студент
Научный руководитель: Богатова И.Б., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

В технологическом процессе химического предприятия образуются сточные воды. В воде остаются вещества, различающиеся по классу опасности, и негативно влияющие на водные экосистемы. Одним из главных факторов, защиты водоемов от загрязнений, является увеличение эффективности функционирования очистных сооружений на предприятиях химической промышленности. Сточные воды должны очищаться и соответствовать нормативам и стандартам. Ужесточение контроля на предприятии за негативным воздействием на окружающую среду требует реконструкции очистных сооружений, которые должны обеспечить требуемое качество очищенных сточных вод.

Актуальность данной проблемы определила цель нашего исследования: модернизация очистных сооружений с уменьшением объема активного ила в цехе 39 по переработке органических и неорганических соединений производства капролактама ПАО «КуйбышевАзот».

Способ биологической очистки заключается в том, что окисление, расщепление и последующее уничтожение органических загрязнений сточных вод, есть результат процесса жизнедеятельности простейших микроорганизмов. На установке нитриденитрификации цеха 39 предусмотрена четырехступенчатая схема очистки сточных вод:

I ступень – нитрификация

II ступень – денитрификация

III ступень – доочистка

IVступень – глубокая доочистка, обеззараживание.

Процесс нитрификации, реализуемый в аэробных зонах аэротенков, представляет собой двухстадийный процесс окисления аммония (NH_4^+) до нитритов (NO_2^-) и, в итоге, до нитратов (NO_3^+).

первая стадия:

$NH_4^+ + 1{,}5\ O_2 \rightarrow NO_2^- + H_2O$

вторая стадия:

$NO_2^- + 0{,}5\ O_2 \rightarrow NO_3^-$

Для реализации процесса нитрификации в ходе очистки сточных вод необходимо обеспечить требуемые:

• время проведения обеих стадий процесса;

• значение аэробного возраста активного ила (рассчитывается в зависимости от температуры сточных вод, качественных и кинетических характеристик поступающих на биологическую очистку сточных вод и требуемого качества очищенной воды, как по аммонийному азоту, так и по азоту нитритов);

• кислородный режим (концентрация растворенного кислорода не должна быть ниже 2 мг/л);

• значение pH не должно быть вне диапазона рабочих значений (6,5–8,5);

• остаточная щелочность не должна быть ниже 50 мг/л по $CaCO_3$.

Процесс денитрификации, реализуемый в аноксидных зонах аэротенков, представляет собой процесс восстановления нитратов (NO_3^-), образованных в ходе процесса нитрификации, до молекулярного азота N_2, который уходит в атмосферу:

органическое вещество + $NO_3^- \rightarrow$ биомасса + CO_2 + N_2

Большинство гетеротрофных микроорганизмов в сооружениях биологической очистки сточных вод могут использовать как растворенный кислород, так и связанный кислород нитратов.

Стадия глубокой очистки денитрифицированного стока предусмотрена для доведения до требований, предъявляемых к качеству повторно используемых сточных вод в системе оборотного водоснабжения завода.

В биореакторах происходит последовательное снижение БПК, ХПК, азота аммонийного и др. загрязнений. Основой доочистки остаточных загрязнений в промышленных стоках является процесс биологического разложения загрязнений на биопленке, которая образуется на пластиковой насадке. Кроме того, на биопленке формируются бактерии нитрификаторы, которые обеспечивают снижение азота аммонийного в сточной воде.

В процессе эксплуатации биореакторов на насадке происходит накопление активного ила, который при его избытке выносится с потоком воды, что увеличивает наличие взвешенных веществ в стоках. Данное состояние отрицательно сказывается на работе Ультрафиолетовой установки и вторичном загрязнении очищенного стока, что способствует биообрастанию на градирнях водооборотных циклов.

В процессе исследования установлено, что существующие сооружения доочистки в биореакторах с прикрепленной микрофлорой не эффективны.

Для решения указанной проблемы рекомендуем технологию очистки сточных вод с использованием мембранных биореакторов (МБР).

Мембранный биореактор сочетает биологическую обработку активным илом с механической мембранной фильтрацией. Мембранный модуль используется для разделения иловой смеси и представляет собой альтернативу широко применяемому методу осаждения активного ила во вторичных отстойниках, используемую в традиционных системах биологической очистки в аэротенках.

Сточные воды, прошедшие предварительную обработку очистку, поступают в распределительный канал, где смешивается с рециркуляционным активным илом. Далее сточные воды поступают в биореактор, в котором последовательно располагаются преаноксидная, аэробная и постаноксидная зоны. Аноксидные емкости оборудованы мешалками.

Аэробные емкости оборудованы мелкопузырчатыми аэраторами, чтобы обеспечить требуемую концентрацию растворенного кислорода (более 2 мг/л), который необходим для окисления органических соединений и для нитрификации. После биологической обработки иловая смесь поступает в рециркуляционную насосную станцию, откуда насосами подается в мембранные емкости. Таким образом, организуется рецикл возвратного ила из мембранных емкостей в аэробную зону. Кроме того, для возврата нитратов дополнительно организуется рецикл (внутренний) из аэробной зоны в преаноксидную.

Преимущества технологии мембранных биореакторов:

1. Возможность произвести, без включения в технологическую схему дополнительных блоков, глубокую очистку сточных вод от загрязняющих веществ до показателей, удовлетворяющих требованиям по сбросу очищенных стоков в природные водоемы всех категорий.
2. Повышение устойчивости работы биореактора к залповым сбросам веществ, характерных для промышленных объектов локального водоотведения.
3. Возможность увеличения или уменьшения производительности без изменения технологического процесса.
4. Снижение на 20–40% массогабаритных характеристик емкостных сооружений, т.к. необходимое количество активного ила находится в меньшем объеме при более высокой концентрации.
5. Получение малого количества избыточного активного ила, что значительно влияет на стоимость его механического обезвоживания и утилизацию.
6. Сокращение на 30–70% площади, занимаемой оборудованием (благодаря отсутствию вторичных отстойников, блоков доочистки, иловых площадок).
7. Обеспечение высокой микробиологической безопасности очищенных стоков.
8. Исключен вынос активного ила из системы в резервуар с очищенной водой.

Библиографический список

1. Постоянный технологический регламент цеха №39 установки нитриденитрификации промстоков производства капролактама №39. Тольятти, 2013-108 с.

2. Поляков, А.М., Соловьев, С.А., Видякин, М.Н. Технология мембранного биореактора (МБР) для очистки природных и сточных вод. ВИНИТИ Серия. Критические технологии. Мембраны, 2008, N°3(39).

ПРЕДЛОЖЕНИЯ К ОРГАНИЗАЦИИ ПРОИЗВОДСТВЕННОГО ЭКОЛОГИЧЕСКОГО КОНТРОЛЯ В ЦЕХЕ № 16 ПАО «ТОАЗ»

Киселева Е., студент
Научный руководитель: Петрякова О.Д., к. т. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Корпорация «Тольяттиазот» является одной из динамично развивающихся, экономически сильных и социально привлекательных компаний отечественной промышленности. Сегодня в состав корпорации «Тольяттиазот» входят крупнейший в мире производитель аммиака «Тольяттинский азотный завод», уникальный завод по изготовлению запасных частей для предприятий химии и нефтехимии «Азотреммаш», региональный банк «Тольяттихимбанк», производители сельскохозяйственной продукции и товаров народного потребления.

Цель работы: повышение экологической безопасности промыщленного объекта, предотвращение аварийных ситуаций и сохранение здоровья работников за счет разработки предложений к плану производственного экологического контроля ТоАЗ для цеха № 16 на складах каустической соды и кислот.

Задачи работы:

1. Выполнить анализ видов, форм и методов экологического контроля;
2. Проанализировать организацию производственного экологического контроля на предприятии;

3) Разработать предложения по производственному экологическому контролю на складах каустической соды и кислот цеха №16 для включения их в план ПЭК ТоАЗа.

Экологический контроль представляет вид государственного управления в сфере экологического права, реализующийся в комплексе мер, направленных на соблюдение общеобя-

зательных норм и правил путем применения норм властного принуждения.

Можно выделить следующие аспекты экологического контроля:

1) Функция государственного управления.

2)Реализация законодательных норм на практике. Г

Виды экологического контроля нашли свое отражение в Федеральном законе от 10 января 2002 года № 7-ФЗ «Об охране окружающей среды»:

а) Государственный экологический контроль.

б) Общественный экологический контроль.

в) Производственный экологический контроль (ПЭК)

ПЭК осуществляется организациями и предпринимателями в ходе хозяйственной деятельности путем разработки и утверждения программы производственного экологического контроля.

Также экологический контроль можно разделить по отдельным видам в зависимости от стадии контроля:

- Предупредительный экологический контроль. Происходит на стадии подготовки к осуществлению хозяйственной деятельности (согласование, проектирование, получение разрешений на допустимый вред окружающей среде и т.д.). Позволяет предусмотреть профилактические меры для недопущения причинения вреда объектам природного мира, а также предотвратить потенциально опасную экологическую деятельность на стадии согласования;

- Текущий экологический контроль. Осуществляется в рамках текущей хозяйственной деятельности и состоит в контроле за хозяйствующими субъектами. Такой контроль заключается в запросе документальной информации, выездных проверках и инспекциях;

- Последующий экологический контроль. Заключается в сборе информации по итогам хозяйственной деятельности, ее обобщении и систематизации с целью дальнейшего регулирования природоохранных мероприятий.

В экологическом праве выделяют следующие формы экологического контроля:

1) Информационный экологический контроль. Реализовывается путем постоянного мониторинга за ситуацией в сфере охраны окружающей среды и позволяет своевременно отслеживать положительные или негативные изменения, как в отношении отдельных объектов природы, так и в экологической ситуации в целом;

2) Карательный (принудительный) экологический контроль. Состоит в применении мер властного принуждения к субъектам, нарушающим нормы экологического права. Привлечение к ответственности осуществляется в пределах установленных санкций[7].

По методам проведения экологический контроль подразделяется на следующие виды:

- Инспекционный экологический контроль. Уполномоченные органы в сфере охраны окружающей среды имеют право проводить инспекции хозяйствующих субъектов на предмет контроля за выполнением норм по охране окружающей среды. В процессе проверки инспекционные органы имеют доступ ко всей разрешительной и технической документации организации;

- Аналитический экологический контроль заключается в анализе информации, полученной в ходе инспекционного контроля, а также обязательной отчетности хозяйствующих субъектов;

- Инструментальный экологический контроль производится путем сбора проб и анализов на предмет причинения вреда объектам окружающей среды и дальнейшего их исследования в лабораторных условиях.

Производственный экологический контроль (ПЭК) является составной частью системы государственного экологического мониторинга. Организация и обеспечение проведения ПЭК полностью возлагается на субъекты хозяйственной и иной деятельности, а наблюдательная сеть его охватывает промышленную площадку, санитарно-защитную зону предприятия. Реализация ПЭК осуществляется на основании специально разработанной программы, определяющей особенности размещения наблюдательной сети, периодичность отбора проб, перечень контролируемых показателей, характер маршрутных обследований, а также состав

отчетной документации, с учетом технологических особенностей проектируемого производства и связанного с этим прогнозируемого уровня воздействия на компоненты окружающей природной среды. Главная цель ПЭК состоит в информационном обеспечении охраны окружающей природной среды на всех стадиях: строительство, эксплуатация и ликвидация объекта.

Цели производственного экологического контроля:

– регулярное получение достоверных данных о текущем состоянии почв, атмосферного воздуха, водных объектов;

– своевременное выявление источников возможных негативных воздействий на качество природной среды;

– контроль за соблюдением согласованных условий природопользования (за уровнем выбросов, сбросов, лимитов размещения отходов);

– информационное обеспечение государственных органов, контролирующих о состоянии окружающей природной среды;

Производственно-экологический контроль в ПАО «ТоАЗ» включает:

1) контроль источников выбросов загрязняющих веществ;

2) контроль уровней загазованности атмосферного воздуха на промышленной площадке и в СЗЗ;

3) контроль уровней и загрязнения подземных вод;

4) контроль сточных вод;

5) контроль воды в Саратовском водохранилище в створе выпуска очищенных сточных вод.

Контроль ведется как за организованными, так и неорганизованными и передвижными источниками выбросов загрязняющих веществ в атмосферу.

ПЭК при аварийных ситуациях отличается высокой оперативностью, а отбор всех видов проб значительно учащается, охватывая участок аварии и прилегающие к нему зоны.

На период эксплуатации работа по охране атмосферного воздуха ведется следующим образом:

1) Контроль за промышленными выбросами загрязняющих веществ в атмосферу от стационарных источников ведется санитарной лабораторией, согласно «Графиков лабораторного контроля промышленных выбросов в атмосферу».

2) На предприятие разработаны «Мероприятия по регулированию выбросов в период неблагоприятных метеорологических условий (НМУ)», которые являются неотъемлемой частью нормативов ПДВ. При наступлении НМУ контроль на промышленной площадке и на границе СЗЗ ведется на машине «Экологическая лаборатория».

3) Для уменьшения выбросов загрязняющих веществ в атмосферу на предприятии работают 18 ПГУ на производствах карбамида, аммиака, КФС, фритты, огнеупоров, метанола, РМЦ. На все ПГУ разработаны и согласованы паспорта. Проверка работы ПГУ ведется следующим образом: 2 раза в год проводится проверка технического состояния ПГУ и 1 раз в год проверка соответствия фактических параметров работы ПГУ проектным. Все проверки оформляются актом с подписью ответственного лица.

4) ПЭК состояния атмосферного воздуха на промышленной площадке, в пределах санитарно-защитной зоны и в населенных пунктах в зоне возможного воздействия (в аварийных ситуациях) может проводиться с помощью передвижной экологической лаборатории и при помощи отбора проб воздуха с учетом розы ветров и результатов предварительного расчета рассеивания допустимых выбросов. Санитарная лаборатория предприятия выполняет данный контроль по «Графику контроля выбросов ЗВ в атмосферу»[10].

5) Ведутся журналы ПОД – 1, 2, 3, предоставляется статистическая отчетность по форме 2 ТП – воздух (за 6 и 12 месяцев текущего года).

6) Проверка технического состояния стационарных источников проводится ежегодно по согласованному графику производственного контроля.

Проводится регулярный контроль за параметрами, техническим состоянием, режимом

работы и соблюдением правил эксплуатации и всех видов оборудования и устройств, работа которых связана со сбросами сточных вод в водные объекты. Контроль качества сточных вод предполагает:

контроль качества стоков в системах канализации на выходе из цехов и на выходе с завода (согласно утвержденному графику);

- контроль качества сточных вод на узле контроля на входе на БОС (согласно утвержденному графику);

- контроль качества очищенных сточных вод на выходе с БОС (согласно утвержденному графику, согласованному с контролирующими органами);

- контроль качества сточных вод абонентов на входе в н/с № 3 (частота).

Состав контролируемых параметров определялся с учетом:

- состава загрязняющих веществ в сточных водах;

- требований природоохранного законодательства к контролю качества окружающей среды.

Периодичность и параметры наблюдений на общем потоке определены в соответствии с графиком аналитического контроля и лицензией на водопользование.

Так как очищенные промышленные стоки сбрасываются в открытых водоем (Саратовское водохранилище), специализированной организацией ведется мониторинг в районе выпуска на створах в водоеме с ежеквартальным предоставлением отчета. Отчеты по мониторингу передаются в «Водное агентство». Основная цель ПЭК поверхностных водных объектов: наблюдения за возможным изменением химического состояния водной среды под воздействием техногенного загрязнения.

В соответствии с имеющимися нормативно-правовыми документами осуществляется наблюдение за образованием, накоплением, временных хранением, транспортировкой, обезвреживанием, утилизацией и захоронением всех видов отходов, образующихся на предприятии должны выполняться требования по раздельному накоплению и временному хранению различных по токсичности отходов, а также по соблюдению безопасности транспортировки опасных отходов. Временное накопление и хранение отходов должно производиться на специально оборудованных площадках с твердым покрытием и защитой от ветра и атмосферных осадков.

Соблюдение правил техники безопасности и экологической безопасности при хранении отходов автотракторной и строительной техники, предусматривает образующиеся в результате ее технического обслуживания отходы собирать и вывозить на свои базы. Крупногабаритный лом черных металлов собирается и хранится навалом на открытой площадке с твердым покрытием. Мелкокусковый лом черных металлов собирается и хранится в металлических контейнерах на той же площадке. Транспортируется лом в открытых транспортных средствах в соответствии с правилами перевозки грузов. Ветошь обтирочная, замасленная накапливается в металлической таре в закрытом помещении или под навесом. Место должно быть оборудовано средствами пожаротушения.

Материалы, получаемые в процессе проведения регулярных системных наблюдений, позволяют оперативно корректировать природоохранные мероприятия и предупреждать аварийные ситуации.

Склад каустической соды (корпус 147) предназначен для приема, хранения и выдачи потребителям каустической соды. Прием сырья производится из ж/д цистерн. Выдача – по трубопроводам. Потребителями сырья являются установки водоподготовки производства аммиака и карбамида.

В зону обслуживания аппаратчика склада каустической соды входит:

- хранилища каустической соды поз. Е-4 / 1-3;
- насос центробежный поз. Н-1 / 1-3-, Н-5 / 1-2;
- вакуумный насос поз. Н-9;
- погружной насос поз. Н-12;
- дренажная емкость поз. Е-7;

- вакуум ловушка поз. Е-6;
- система приточной и вытяжной вентиляции;
- система отопления;
- оборудование КИПиА со щитами в операторной;
- сливная эстакада, помещение насосной, поддоны сливной эстакады и хранилищ;
- трубопроводы сливной эстакады, насосной, хранилищ и МЦК до первых задвижек потребителей;
- система обогрева оборудования и трубопроводов на складе МЦК;
- система водоснабжения в пределах корпуса 147;
- система канализации, неорганических загрязнителей, хозбытовых стоков.

Приходящие на завод цистерны с каустической содой при минусовых температурах подаются тепловозом в тепляк под одну из трех точек слива на сливной эстакаде.

Склад кислот (серная и соляная, корпус 185) предназначен для приема, хранения и выдачи потребителям кислот. Прием сырья производится из ж/д цистерн. Выдача – по трубопроводам. Серная кислота пожаро-, взрывобезопасна, пары токсичны. Серная кислота и олеум при попадании на кожу человека вызывает сильные, долго не заживающие химические ожоги. Мелкие брызги при попадании в глаза могут вызвать потерю зрения. Вдыхание концентрированных паров серной кислоты вызывает раздражение верхних дыхательных путей.

ПДК паров серной кислоты в воздухе рабочий зоны – 1мг/м^3.

Кислота соляная техническая хорошо растворима в воде. Туман соляной кислоты сильно раздражают верхние дыхательные пути и слизистые оболочки глаз. Длительное воздействие может вызывать катар дыхательных путей, помутнение роговицы глаз. При воздействии на кожу вызывает ожоги и изъязвления.

При поступлении на склад цистерн с продуктом в жидком виде, процесс откачки осуществляется без разогрева цистерны паром.

Как видно из вышеизложенного, в цехе №16 особую опасность представляют кислоты и щелочи, необходимо контролировать их возможную утечку и качество воздуха рабочей зоны. Однако в заводской план ПЭК данное подразделение не вошло. Разработаем мероприятия для осуществления ПЭК в цехе №16.

Предлагается метод турбидиметрического определения аэрозоля серной кислоты в воздухе склада кислот по стандартной методике.

Согласно графику аналитического контроля воздушной среды и физических факторов, отбор проб воздуха на предприятии производится один раз в месяц.

В ходе исследования выяснилось, что ПЭК на складах каустической соды и кислот не проводится. Сточных вод, в процессе откачки и хранения кислот и щелочей потребителю, не образуется. Только бытовые воды в ходе использования душевых и туалета. Шум и вибрации незначительные. Поскольку других вредных факторов воздействия на окружающую среду в данных корпусах нет, то контроля по загрязнению воздуха будет достаточно.

Предлагается организовать ПЭК в цехе №16 по следующему плану, представленному в таблице 1.

В зимнее время, прибывшие цистерны с каустической содой, требуется обогреть паром 8-10 часов перед началом откачки, что увеличивает вероятность нахождения в воздухе аэрозолей остронаправленного действия. Соответственно, предлагаем производить ПЭК зимой в два раза чаще (два раза в неделю) в местах расположения наливной и сливной эстакады, так как обогрев производится именно под точками слива.

Таблица 1 - Порядок проведения ПЭК в цехе №16

№ п/п	Место отбора проб воздуха	Периодичность	Ответственное лицо	Кем проводится отбор
1	Насосная	1 раз в 2 недели	Инженер по ПЭК	Лаборантом
2	Центральный пульт управления (ЦПУ)	1 раз в месяц	Инженер по ПЭК	Лаборантом

3	Наливная и сливная эстакада, точки слива	1 раз в неделю	Инженер по ПЭК	Лаборантом
4	Поддоны хранилищ кислот и щелочей	1 раз в 2 недели	Инженер по ПЭК	Лаборантом
5	Трубопровод в местах расположения запорно-регулирующей арматуры	1 раз в месяц	Инженер по ПЭК	Лаборантом

Производственный экологический контроль позволит в короткие сроки выявить превышение ПДК. Материалы, получаемые в процессе проведения регулярных системных наблюдений, позволяют оперативно корректировать природоохранные мероприятия и предупреждать аварийные ситуации. В случае если превышения по ПДК будут учащаться, то возможно рассмотреть обновление вентиляционных систем, замену запорно-регулирующей арматуры, внедрить сигнализации, оповещающие о чрезмерном загрязнении воздуха.

Библиографический список

1. Типовая инструкция по организации системы контроля промышленных выбросов в атмосферу в отраслях промышленности. Госкомгидромет, ГГО

2. Федеральный закон Российской Федерации «Об охране окружающей среды» от 10 января 2002г. № 7-ФЗ, Статьи 64 и 67.

АНАЛИЗ МЕТОДОВ ОЧИСТКИ СТОЧНЫХ ВОД ОТ ФОСФАТОВ

Сорочинская В.Д., магистрант
Научный руководитель: Селезнев В.А., д. т. н., профессор
Тольяттинский государственный университет
г. Тольятти

Вода – важнейшая составляющая жизни на земле в целом и здоровья человека в частности. Активные темпы развития промышленных предприятий и городских территорий способствуют возрастанию антропогенной нагрузки на природные водоемы. Основным источником загрязняющих веществ, поступающих в водоемы и водотоки, являются сточные воды. Содержащиеся в стоках биогенные вещества, такие как фосфаты, активизируют процессы антропогенного эвтрофирования водоемов и приводят к ухудшению качества природных вод в целом.

В природных условиях процесс эволюции водоема занимает длительное время. Однако в условиях антропогенной нагрузки скорость старения водоемов существенно увеличивается. В первую очередь это связано с поступлением в природные водоемы большого количества биогенных веществ со сточными водами. Как правило, элементами, лимитирующими производство первичной продукции водоемов, являются азот, фосфор и их соединения, особенно фосфор.

Основным антропогенным источником фосфора и его соединений в водоемах, как правило, являются хозяйственно-бытовые сточные воды. Бурное развитие производства моющих средств и практически повсеместное использование стиральных машин-автоматов в быту привело к увеличению в составе сточных вод концентрации биогенных веществ, в частности фосфатов.

Еще одним источником поступления в водоемы соединений фосфора является промышленность по производству минеральных удобрений, которая переводит фосфор из недоступных для микроорганизмов форм, таких как апатиты, в доступные формы – фосфаты.

В настоящее время в сфере очистки сточных вод от соединений фосфора существует большое разнообразие методов, которые можно выделить в три основных группы [1; 2; 3]:

– химический и физико-химический;

– биологический;
– биолого-химический.

В настоящее время удаление фосфора химическим и физико-химическим способами ограничено. Эти методы имеют высокую экономически невыгодную ресурсо- и энергоемкость, а также могут нести за собой вторичное загрязнение сточных вод. Тем не менее, такие методы очистки сточных вод от фосфатов находят свое применение на стадии доочистки сточных вод.

Большое распространение на современном этапе получил биологический метод удаления фосфора, основанный на связывании фосфора микроорганизмами активного ила в результате их жизнедеятельности. Суть метода заключается в последовательном проведении сточной воды через три зоны: анаэробную, бескислородную и аэробную.

Однако в большинстве случаев, применяя только биологические методы, не удается достичь такого уровня нормативных требований ПДК по содержанию фосфатов в сточной воде для водоёмов рыбохозяйственного значения. Поэтому на практике распространены различные схемы, сочетающие в себе биологическое очищение и химическое осаждение (например, на Центральной станция аэрации (ЦСА) в Санкт-Петербурге) [7; 8]. Такое совмещение методов позволяет добиться более высокого качества очищения воды, чем при применении каждого из них.

Также происходит и совершенствование реагентов, применяемых для биохимической очистки сточных вод от фосфатов. Перспективным являются использование реагентов, состоящих из отходов производств, например осадки водопроводных станций, экстракты золы бурого угля, отходы производства железа и т. д. Так, известна технология очистки промышленных и бытовых стоков от соединений фосфора с использованием белого шлама (БШ) - оборотного продукта глиноземного производства в виде порошка [5].

Неплохие результаты показала методика очистки фосфат содержащих водных сред при помощи отхода электросталеплавильного производства, основанная на осаждении образующегося в результате реакции фосфата кальция [6].

В настоящее время проблема очищения сточных вод от фосфатов не имеет оптимального решения и требует дополнительных исследований и разработок. Применяющиеся биологические методы не позволяют достичь требуемой санитарным законодательством степени очистки от соединений фосфора, а физико-химические методы, несмотря на довольно хорошие результаты по степени очистки, требуют значительных экономических затрат и создают дополнительную проблему в виде необходимости обработки осадков, образующихся при реагентной обработке [4].

Библиографический список

1. Харькина, О.В. Эффективная эксплуатация и расчет сооружений биологической очистки сточных вод. - Волгоград: изд-во «Панорама», 2015. –433 с.

2. Разумовский, Э.С. Современные технологии очистки сточных вод // Жилищное и коммунальное хозяйство. – 1994. – №3. – С. 30-34.

3. Саблий, Л.А. , Жукова, В.С., Козарь, М.Ю. Удаления соединений азота и фосфора: проблемы и их решения // Сборник статей 5ой Восточно-Европейской конференции «Опыт и молодость в решении водных проблем» IWA. Часть 2. (Русскоязычная версия). - Киев, 26-28 июня 2013г. - стр. 351-358.

4. Бураев, М.Э., Кольздорф, А.В., Котомцев, В.В., Луцкая, Л.П., Луцкий, Р.А., Устич, Е.П. Патент на изобретение №: 2440304 Способ очистки сточных вод от соединений фосфора. - [Электронный ресурс]. - Режим доступа: http://bankpatentov.ru/node/191246

5. Свергузова, С.В. Василенко, Т.А. Очистка сточных вод от фосфатов с помощью шлаков Оскольского электрометаллургического комбината // Наука производству. - 2001, № 3. - с. 13-17.

6. Крючихин, Е.М., Николаев, А.Н., Жильникова, Н.А., Рублевская, О.Н., Панкова, Г.А., Рафалович, Г.Н. Эффективная очистка городских сточных вод от биогенных

элементов на ЦСА Санкт-Петербурга // Водоснабжение и санитарная техника. – М., 2009. - №12 — стр. 59-62.

7. Васильев, Б.В., Мишуков, Б.Г., Соловьева, Е.А. Реагентное удаление фосфора из городских сточных вод // Водоснабжение и санитарная техника. - 2009. - N 2. - С. 58-60.

8. Sukalyan Sengupta, Tabish Nawaz, Jeffrey Beaudry. Nitrogen and Phosphorus Recovery from Wastewater. Current Pollution Reports 1:3. - 2015. - S. 155-166.

РОСТ И РАЗВИТИЕ РАСТЕНИЙ ФАСОЛИ И СОИ ПРИ СОВМЕСТНОМ ВЛИЯНИИ ВНЕШНИХ ФИЗИЧЕСКИХ ПОЛЕЙ И ИОНОВ КАДМИЯ

Тареева А.А., магистрант
Научный руководитель: Ольшанская Л.Н., д. х. н., профессор
Саратовский государственный технический университет имени Ю.А. Гагарина
г. Саратов

Площадь загрязненных земель в России достигла более 70 млн. га, из них около 1 млн га имеют чрезвычайно опасный уровень загрязнения. Загрязнение почвы носит глобальный характер и может привести к непоправимым последствиям. Разрушение плодородного слоя неумолимо ведет к нарушению природного баланса, обмена веществ в природе. Загрязнение почвы может обернуться разрушением и других экосистем, поэтому в стране необходимы срочные меры по снижению уровня загрязнения почв, особенно тяжелыми металлами (ТМ). Загрязнение почв ТМ имеет сразу две отрицательные стороны. Во-первых, поступая по пищевым цепям из почвы в растения, а оттуда в организм животных и человека, они вызывают серьезные заболевания, ведут к сокращению продолжительности жизни, а также к снижению количества и качества урожаев сельскохозяйственных растений и животноводческой продукции. Во-вторых, накапливаясь в почве в больших количествах, ТМ способны изменять многие ее свойства. Прежде всего, изменения затрагивают био-логические свойства почвы: снижается общая численность микроорганизмов, сужается их видовой состав (разнообразие), изменяется структура микробо-ценозов, падает интенсивность основных микробиологических процессов и активность почвенных ферментов и др. Сильное загрязнение ТМ приводит к изменению и более консервативных признаков почвы, таких как гумусное состояние, структура, pH среды и др. Результатом этого является частичная, а в ряде случаев и полная утрата почвенного плодородия [1].

В последние десятилетия обнаружены многочисленные факты, свидетельствующие о высокой чувствительности растений к воздействию внешних физических полей различной природы (ВФП: УФ-, ИК-излучение, магнитные поля и др.), которые создают дополнительные электрические токи в биообъектах, и, изменяя величины мембранного потенциала клетки, могут управлять течением процессов роста и развития, оказывая как стимулирующее, так и тормозящее влияние. Это воздействие зависит от характеристик внешних физических полей: длины волны, частоты колебаний электромагнитных излучений, интенсивности и времени [2, 3]. Такая обработка семян является прогрессивным способом их подготовки к посеву, позволяющим не только вывести семена из состояния покоя, но и активизировать работу разнообразных биологических катализаторов – ферментов, обеспечивающих быстрый рост и развитие растений. В клеточной стенке имеются белки, пектины, фосфолипиды и др., содержащие фиксированные отрицательно заряженные группы (прежде всего – карбоксильные). Они определяют катионно-обменную способность и влияют на накопление катионов ТМ в клетке из почвенного раствора высшими растениями в процессе фиторемедиации, уменьшая количество поллютантов в почве [4].

В работе исследованы процессы роста и развития растений сои и фасоли в процессе очистки почв от ионов кадмия методом фиторемедиации при воздействии на семена фитомелиорантов (соя и фасоль) УФ- излучением и постоянным магнитным полем (ПМП).

Тестовые культуры (фиторемедианты) - соя (*Glycine max*) сорт Самер 2 и зерновая красная

фасоль (*Phaseolus vulgaris*) сорт Рубин, районированы в Саратовской области. Выбор обусловлен тем, что в целях фиторемедиации обычно используют высокопродуктивные культуры. Загрязняющими веществами служили растворы $3CdSO_4 \cdot 8H_2O$ с концентрацией катионов Cd^{2+} 5 и 15 ПДК для почвы (ПДКCd=1 мг/кг почвы). В качестве источника УФ-излучения выступала бактерицидная лампа, марки СБПе 3х30 Вт, с длиной волны $\lambda = 257$ нм; источником постоянного магнитного поля (ПМП) с напряженностью 2 кА/м служил прибор марки Б5-43. Обработку семян проводили при выбранном времени в течение 6 часов [3]. Результаты проведенных исследований по влиянию кадмия в различных концентрациях и воздействий УФ-облучения и ПМП на количество всходов семян сои представлены в таблице 1.

Таблица 1 - Влияние концентрации кадмия и воздействий ВФП на количество всходов семян сои (от 15 семян)

Сутки	Количество всходов, штук				
	Контроль	Воздействие ультрафиолета, 6 ч.		Воздействие ПМП, 6 ч.	
		5 ПДК	15 ПДК	5 ПДК	15 ПДК
7	8	6	4	6	3
14	10	6	6	6	7
21	10	7	8	6	7
28	9	6	7	6	7

Установлено, что по сравнению с контролем количество всходов в почвах, содержащих катионы кадмия, отличалось от количества всходов в контрольном образце. Так, по сравнению с контролем, в почвах, содержащих кадмий, при концентрациях 5 и 15 ПДК всхожесть семян сои, обработанных УФ облучением и ПМП в течение 6 часов практически всегда была меньше.

Проведенные исследования по влиянию концентрации кадмия и воздействий УФ-облучения и ПМП в течение 6 ч на количество всходов семян фасоли представлены в таблице 2.

Таблица 2 - Влияние концентрации кадмия) и воздействий УФ и ПМП на количество всходов семян фасоли (от 15 семян)

Сутки	Количество всходов, штук				
	Контроль	Воздействие ультрафиолета, 6 ч.		Воздействие ПМП, 6 ч.	
		5 ПДК	15 ПДК	5 ПДК	15 ПДК
7	0	5	3	4	
14	4	7	6	5	
21	5	8	6	5	
28	5	6	6	5	

Количество всходов фасоли, обработанной УФ облучением и высаженной в почвы, содержащие кадмий в концентрациях 5 и 15 ПДК, по сравнению с контролем увеличилось. При воздействии ПМП и кадмия в концентрации 5 ПДК количество всходов оказалось равным количеству всходов семян в контрольном образце, а при концентрации Cd^{2+} 15 ПДК, количество всходов снизилось.

Средняя высота растений фасоли при воздействии Cd^{2+} и ВФП на 28 сутки представлена на рисунке 1.

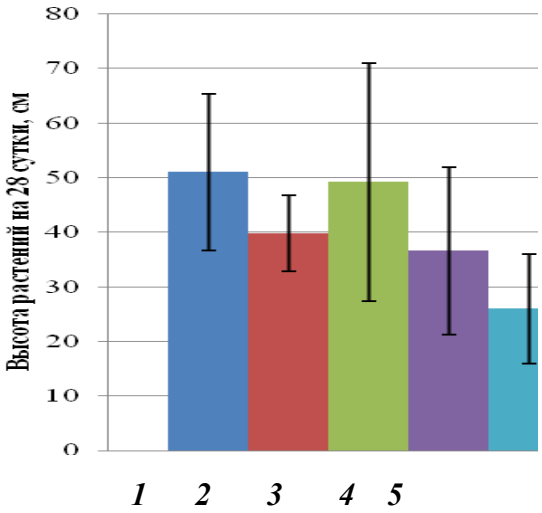


Рисунок 1 - Средняя высота растений фасоли при воздействии ВФП и ионов Cd^{2+} на 28 сутки:
1 – 5 ПДК+ПМП; 2 - 15 ПДК+ПМП;
3 - 5 ПДК+УФ; 4 – 15 ПДК+УФ; 5 – контроль (без ВФП и ТМ)

ВЫВОДЫ

1. Изучено влияние содержания кадмия на процессы всхожести семян, роста и развития растений сои и фасоли. Установлено, что с увеличением концентрации катионов ТМ в почве, сильнее проявляется их токсическое действие.

2. Показано, что воздействие УФ и ПМП в течение 6 ч. на семена сои в присутствии кадмия в концентрации 5 и 15 ПДК стимулировали всхожесть, рост и развитие растений.

3. Анализ полученных данных показал, что кадмий не оказывает сильного токсического воздействия на рост и развитие растений. Это вероятнее всего обусловлено тем, что, не являясь микроэлементом, необходимым для роста и развития растений, токсикант кадмий, фиксируется в основном в вакуолях или межклеточном пространстве и его концентрация в фитомассе не контролируется.

Библиографический список

1. Вальков, В.Ф. Экология почв: учебное пособие для студентов вузов. Ч. 3. Загрязнение почв / В.Ф. Вальков, К.Ш. Казеев, С.И. Колесников. - Ростов-на-Дону: УПЛ РГУ, 2004.- 54 с.

2. Взаимодействия физических полей с живым веществом: монография / Е.И. Нефёдов, А.А. Протопопов, А.И. Семенцов, А.А. Яшин / Под общей редакцией А.А. Хадарцева.- Тула: ТГТУ. - 1995.- 98 с.

3. Влияние природы и концентрации ионов металлов и совместное влияние ИТМ и внешних физических полей на процессы роста и развития растений / Л.Н. Ольшанская, А.С. Халиева, О.В. Титоренко // «XXI век: итоги прошлого и проблемы настоящего плюс»: Научно-технический журнал 2014. -№ 01 (17).- С. 125 - 131.

4. Опритов, В.А. Непосредственное сопряжение генерации потенциала действия в клетках высшего растения Cucurbitapepo L. с работой электрогенного насоса / В.А. Опритов, С.С. Пятыгин, В.А. Воденеев // Физиология растений.- 2002.- Т.49, № 1. - С.160-165.

ПРИМЕНЕНИЕ ОТХОДОВ СТАЛЬНОЙ ОКАЛИНЫ ДЛЯ ИЗГОТОВЛЕНИЯ МАГНИТОСОРБЕНТОВ

Чернова М.А., магистрант, Баканова Е.М., аспирант
Научный руководитель: Ольшанская Л.Н., д. х. н., профессор
Саратовский государственный технический университет имени Ю.А. Гагарина
г. Саратов

Введение. Нефтепродукты и пластовые воды являются приоритетными загрязнениями окружающей среды. Выброшенные на поверхность пластовые воды изменяют микрорельеф территории и являются источниками вторичного засоления почв вокруг скважин. Они являются полиингридиентными полютантами, обладающими высокой геохимической активностью и токсичностью. В их составе присутствуют нефтяные углеводороды, разнообразные соли и механические примеси, которые, поглощаясь почвой и, поступая в грунтовые воды, резко изменяют их химические и физико-химические свойства – солевой состав, щелочность, реакцию почвенных суспензий, нарушают водно-воздушный режим и углеродно-азотный баланс [1]. Ущерб от крупномасштабных разливов нефти трудно подсчитать и оценить его зависимость от вида Н и НП, состояния пострадавшей экосистемы, погоды, океанских и морских течений, времени года, состояния местного рыболовства и туризма и др. Очистка водных сред от продуктов нефтепереработки имеет свою специфику, так как, изначально, это вещества органического происхождения, обладающие некоторыми свойствами такими как: вязкость, низкая либо высокая плотность, летучесть и др. Таким образом, уместно использовать различные методы, позволяющие извлекать данные поллютанты с различной степенью эффективности.

При проведении мероприятий по ликвидации разливов Н и НП с поверхности водных сред или почв особый интерес представляют недорогие, эффективные методы очистки, к которым относятся сорбционные. С их помощью возможно удаление загрязнений весьма широкой природы практически до любой остаточной концентрации независимо от их химической устойчивости, отсутствие вторичных загрязнений и управляемость процессом. Преимуществами сорбционных методов является также их совместимость с другими способами сбора нефтепродуктов, возможность многократного использования сорбента после регенерации. При выборе материалов следует учитывать их экологичность, а также доступность в регионе. Использование различных адсорбентов для сбора Н и НП с поверхности водных сред позволяет достичь очистки до 98 %. В последнее время для этих целей широкое применение находят магнитные сорбенты, которые обладают важным технологическим преимуществом - возможности быстрого и эффективного извлечения нефтезагрязнений из очищаемой среды с помощью магнитного поля. Авторами [2] разработаны сорбенты с магнитными свойствами на основе ферритизированного гальваношлама (размер частиц 41 – 66 нм) для ликвидации разливов нефти и нефтепродуктов.

В целом следует отметить, что предотвращение загрязнения окружающей среды нефтью и продуктами ее переработки –это одна из сложных и многоплановых проблем охраны природной среды.

Цель настоящей работы заключалась в разработке нового магнитосорбента (МС) на основе отходов окалины металлической пыли для очистки загрязненных вод от нефти и нефтепродуктов и минимизации негативного воздействия предприятий нефтехимического профиля на гидросферу.

Экспериментальные данные и их обсуждение. Объектами исследования служили: 1 - отработанное машинное масло марки «Motul»; 2 - нефть с предприятия ПАО «Саратовский НПЗ»; 3 - модельные системы воды с пленками нефти и НП на ее поверхности; 4 - отходы стальной пыли (СО, окалина) ОАО «Трансмаш» (г. Энгельс) после обработки стальных изделий на машине плазменной резки – «Кристалл»; 5 - парафин (ПФ).

Был изготовлен и исследован магнитосорбент состава МС - СО:ПФ = 1:1.

Установлен элементный состав стальной окалины (таблица 1) с использованием рентгенофлуоресцентного спектрометра «Спектроскан Макс» фирмы СПЕКТРОН (Россия, Санкт-Петербург).

В наибольшем процентном соотношении в составе СО содержится железо Fe≈67 %, в незначительных количествах присутствуют: Si, Mn, Al, и др. Это указывает на высокие магнитные свойства материала для изготовления композиционного магнитного сорбента.

Таблица 1 –Элементный состав пыли

Компонент	Массовая доля, %	Погрешность, %	Элемент	Массовая доля, %	Погрешность, %
Fe_2O_3	95,38000	0,11000	Fe	66,71000	0,07000
SiO_2	2,00000	0,07000	Si	0,93300	0,03300
MnO	1,09000	0,05000	Mn	0,84700	0,04000
Al_2O_3	0,47800	0,02400	Al	0,25300	0,01300

Определение токсичности стальной окалины СО проводили согласно методикам [3,4]. В качестве тест - объектов использовали культуры рачков *Daphnia magna* и водоросли *Scenedesmus quadricauda* (рисунок 1). Установлено, что в исследуемой воде выживаемость дафний составила 100 %. Определение острого токсического действия вытяжки на водоросли определяли по снижению уровня флуоресценции хлорофилла зеленых протококковых водорослей *Scenedesmus quadricauda* (*Turp*.) *Breb*.

Полученные данные показали, что водная вытяжка не оказывает острого токсического действия на водоросли. Установлено, что биотестирование на двух тест объектах показало нетоксичность пыли и она может быть использована в качестве компонента магнитосорбентов. На основании приказа Минприроды РФ № 536 от 04.12.2014 г., отход может быть отнесен к V классу опасности [5].

а б

Рисунок 1 – Тест – объекты: а - Daphnia magna; б - Scenedesmus quadricauda

Для изготовления сорбционных материалов (СМ) отходы пыли направляли в смеситель, где смешивали с предварительно расплавленным (45-60 ^{0}C) парафином. После смешения смесь с парафином охлаждали до застывания, а затем измельчали (рисунок 2).

Полученные сорбенты представляют собой мелкодисперсный порошок и могут быть выполнены в виде хлопьев или гранул с размером 0,5-3,0 мм. Выбор парафина как связующего обусловлен его физико-химическими свойствами: плотность 0,880-0,915г/см³ (при 15 ^{0}C) меньше плотности воды, гидрофобность, инертность к большинству химических реагентов, нерастворимость в воде, температура плавления в диапазоне 45 - 65 ^{o}C. Это вещество белого цвета с молекулярной массой 300-450, в расплавленном виде обладающее низкой вязкостью, получают главным образом из нефти.

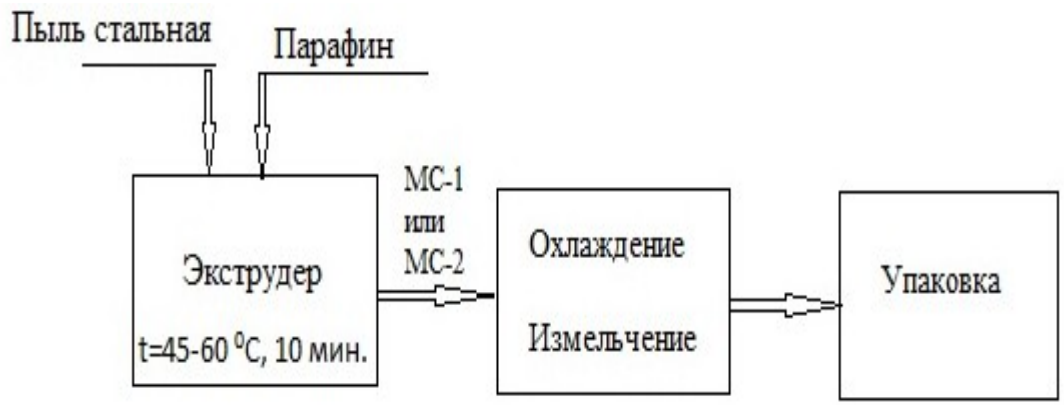
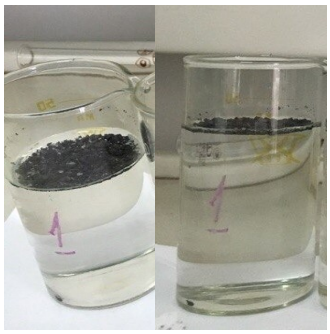


Рисунок 2 – Технологическая схема получения мангитосорбентов

Для выбора рационального состава МС исследовали их физико-химические и сорбционные свойства. **Плавучесть** МС определяли в течение 96 часов с контролем через каждые 24 ч. В результате была установлена 98 % плавучесть сорбента (рисунок 3). Благодаря гидрофобности парафина, магнитосорбенты длительно оставались на поверхности воды, что позволяет создать необходимый резерв времени для ликвидации аварийных разливов нефти и ее продуктов и извлечения сорбента с поглощенным поллютантом.



а б

Рисунок 3 - Плавучесть МС спустя: а - 24 ч.; б - 96 ч.

Смачиваемость является основной характерис-тикой гидрофобных материалов. Её определяли путем измерения краевых углов смачивания сидящей капли воды на поверхности сорбента. Исследуемые сорбенты насыпали на фильтровальную бумагу, затем на поверхности сорбентов наносили воду, фотографировали по профилю и определяли угол смачивания сорбента. Его величина составила 128^{o}, что больше 90^{o} и указывает на гидрофобность материала. В аналогичных экспериментах отработанное машинное масло и нефть сразу впитывались магнитосорбентами не образуя сидящей капли, что свидетельствует об их олеофильности. Для установления **водопоглощения** образцы МС взвешивали и помещали в испытательный контейнер объемом 1 $дм^3$, наполовину заполненный водой и установленный на магнитную мешалку. Через 15 минут образцы извлекали, взвешивали, и рассчитывали водопоглощение. Установленная низкая величина водопоглощения ~0,126 г/г, подтвердили гидрофобность и позволяют рекомендовать материал для изготовления сорбентов.

Нефтеемкость МС (НЕ, г/г) определяли по разнице начальной массы сухого сорбента (m_c=0,5 г), помещенного в упаковку из капрона (m_0=0,5 г) до и после контакта с машинным маслом (интервал 5 мин.) и последующего полного стекания избыточного количества нефтепродуктов:

Полученные результаты представлены на рисунке 4.

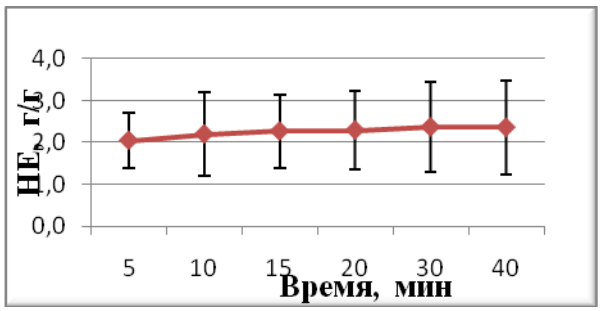


Рисунок 4 - Изменение нефтеемкости МС во времени

Поглощение нефтепродуктов сорбентом является сложным процессом, включающим такие явления, как адсорбция, адгезия, капиллярные явления, заполнение межзёренных пространств.

Полученные усредненные данные по сорбции машинного масла и нефти магнитосорбентом в зависимости от толщины пленки Н или НП на поверхности воды представлены в таблице 3. По завершении процесса сорбции нефти и НП сорбентами, поглощенные вещества извлекаются методом центрифугирования или на вакуум-фильтрах. Это позволяет повторно использовать НП в промышленности, регенерировать сорбенты и повторно использовать. По истечении способности к сорбции/десорбции (после ~ 5-7 циклов регенерации) материалы подвергаются утилизации, например, пиролизом с получением тепловой энергии или в качестве смолистых добавок в асфальтовые смеси при производстве дорожных покрытий.

При этом порошок отходов стальной металлической пыли, образующийся на конечной стадии пиролиза, может быть вновь возвращён в процесс получения магнитосорбентов.

Таблица 3 – Влияние толщины пленки на сорбцию (г/г) Н и НП сорбентом

Толщина пленки, мм	масло	нефть
0,5	1,51	2,09
1,5	3,69	4,93
2,5	5,67	6,55
3,5	8,24	9,24

ЗАКЛЮЧЕНИЕ

1. Установлен элементный состав стальной окалины, содержащей ≈67% железа, что указывает на высокие магнитные свойства материала и возможность получения магнитосорбента на ее основе для очистки загрязненных вод от нефти и нефтепродуктов.

2. Биотестирование на двух тест объектах (рачки *Daphnia magna* и водоросли *Scenedesmus quadricauda*) позволило установить, что отходы стальной пыли не токсичны и могут быть использованы в качестве компонента магнитосорбентов.

3. Разработан состав и способ изготовления магнитосорбента на основе отходов производства – окалины стальной пыли со связующим парафином и исследованы его физико-химические свойства. Установлена высокая гидрофобность - краевой угол смачивания 128^{o}; плавучесть материала в течение 96 ч. составила 98 %; сорбенты показали низкое водопоглощение 0,126 г/г и удовлетворительную нефтеёмкость 2,1 ± 0,26 г/г.

4. Показано, что сорбционное равновесие достигается за первые 10 - 20 мин. контакта материала с Н и НП, на сорбцию оказывает влияние природа и толщина слоя нефтепродуктов. Максимальная сорбционная емкость достигается при толщине пленки 3,0 ± 0,5 мм.

Библиографический список

1. Демельханов, М.Д. Экологические последствия разливов нефти / М.Д. Демельханов, З.П. Оказова, И.М. Чупанова // Успехи современного естествознания. – 2015. – № 12. – С. 91 – 94.

2. Разработка сорбента с магнитными свойствами на основе гальваношлама для ликвидации

разливов нефти и нефтепродуктов / И.Н. Долбня, Е.А. Татаринцева, Е.А. Бухарова, Л.Н. Ольшанская // Химическое и нефтегазовое машиностроение. - 2018. - № 4. - С.42 – 44. ISSN 0023-1126.

3. Методика определения токсичности воды и водных вытяжек из почв, осадков сточных вод, отходов по смертности плодовитости дафний [текст]: Федеральный реестр. – М.: Акварос. - 2007. – 35 с.

4. Методика определения токсичности воды и водных вытяжек из почв, осадков сточных вод и отходов по изменению уровня флуоресценции хлорофилла и численности клеток водорослей [текст]: Федеральный реестр. – М.: Акварос. -2007. –35 с.

5. Об утверждении критериев отнесения отходов к I–V классам опасности по степени негативного воздействия на окружающую среду [текст]: приказ Минприроды России № 536 от 4 декабря 2014 г.

ПРОБЛЕМЫ РАЗВИТИЯ СВОБОДНЫХ ЭКОНОМИЧЕСКИХ ЗОН В РОССИИ

Абдалова А.А., студент
Научный руководитель: Щукина А.Я., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Свободные экономические зоны успешно действуют во всех странах мира. Они функционируют как в промышленно развитых странах, так и в развивающихся.

Помимо привлечения иностранного капитала, задействованного для активизации экономических процессов внутри страны, создание производственных свободных экономических зон увязывают с тремя основными задачами: стимулирование промышленного экспорта и получение на этой основе валютных средств, рост занятости, превращение зон в полигон по опробованию новых методов хозяйствования, полюса роста национального хозяйства. Всё это позволяет укреплять экономическую безопасность как регионов, так и государства в целом.

СЭЗ имеют множество названий, но в мировой практике общепризнанным является термин «свободные экономические зоны». В российском же законодательстве закреплено понятие «особых экономических зон».

22 июля 2005 года был принят Федеральный закон № 116 «Об особых экономических зонах в Российской Федерации». В 2006 году для реализации законопроекта было создано ОАО «Особые экономические зоны», 100% акций которого принадлежит государству. Но важно отметить, что инфраструктурные условия и налоговые льготы в России имеют гораздо меньшую привлекательность, по сравнению с зарубежными аналогами[1].

Развитие ОЭЗ в России происходит крайне непоследовательно. Например, туристические зоны в Калининградской области и Краснодарском крае были закрыты из-за отсутствия резидентов. При этом желающие стать резидентами были, но местные власти и бизнес не смогли договориться. Тяжело идет развитие транспортных ОЭЗ в России: аэропортовая зона «Ульяновск - Восточный» смогла найти нескольких резидентов только после полутора лет переговоров. В портово-логистических зонах в Хабаровском крае и Мурманске резидентов по-прежнему нет. Первую из них даже собирались закрыть, однако в итоге правительство приняло решение расширить зону, включив в нее и порт Ванино. Оказалось, что проект в Мурманске изначально имел слабое экономическое обоснование: Байкало-Амурская магистраль, заканчивающаяся в ОЭЗ «Советская Гавань», не могла пропустить столько грузов, сколько закладывалось в проекте[2].

Большинство российских ОЭЗ себя не оправдали: они просто стали очередным очагом неэффективного расходования бюджетных средств. А промышленные зоны, в которых производится в основном сборка зарубежной техники, быстро окупаются, и, скорее всего, они бы заработали и без всяких льгот. Что же касается других типов ОЭЗ, то они оказались неуспешными по причине отсутствия серьезной проработки проектов. Именно так обстоят дела с портовыми ОЭЗ, многие туристические зоны, которые широко анонсировались, в реальности появились лишь в нескольких регионах.

Проблемы функционирования и невысокая эффективность особых экономических зон в России вызваны многими причинами.

Во-первых, в РФ определена слишком жесткая типизация ОЭЗ, что сильно ограничивает возможности формирования эффективных кластеров. Например, инновационная экономи-

[1] Сайт Россия. Особые экономические зоны [Электронный ресурс]. – Режим доступа: http://www.russez.ru, дата обращения: 26.11.2018.

[2] Сайт Русская планета [Электронный ресурс]. – Режим доступа: http://rusplt.ru/sub/economy, дата обращения: 18.10.2018.

ка подразумевает тесную связь научно-технических разработок и производства, но эти виды деятельности предлагается осуществлять в различных ОЭЗ (технико-внедренческой и промышленно-производственной соответственно). Существует негласное правило, согласно которому региону нежелательно предоставлять более одной особой экономической зоны.

Во-вторых, по мировым меркам российские ОЭЗ обладают относительно малыми налоговыми льготами, поэтому не очень привлекательны для глобальных инвесторов. Фактически государство снижает только региональные и местные налоги, что делаетэтот инструмент менее интересным для субъектов Федерации. В то время как резиденты зарубежных ОЭЗ имеют и другие виды поддержки. Им оказывается консультационная помощь, обеспечивается централизованный маркетинг и связи с общественностью, предоставляется льготное кредитование. В некоторых случаях могут вводиться даже специальные тарифы на ресурсное обеспечение.

В-третьих, проблемы создают слишком большие размеры территорий ОЭЗ. Зонами внушительных масштабов крайне тяжело эффективно управлять и обеспечить им необходимый контроль, к тому же для их инфраструктурного обустройства требуютсясолидные капиталовложения, которые государство не всегда в состоянии обеспечить[1].

Существуют несколько необходимых условий привлечения резидентов на ОЭЗ. Во-первых, нужно обозначить сегменты промышленности, также типы производств, которые окажутся наиболее предпочтительными. Этим типам должны подходить географическое положение, инфраструктура, особенности менеджмента и деловые связи. Во-вторых, важно определить вероятные типы производств, в случае возникновения близких к основным типам предложений.

Так, регионы, привлекая к себе инвесторов, должны отдавать себе отчет в том, что необходимо четко обозначить систему налоговых льгот и механизмов их получения, чтобы обеспечить инвестора благоприятными условиями его деловой активности. Стоит отметить, что нужно направить работу налоговых органов на содействие инвесторам, получившим льготы от руководства региона, включая федеральные. Даже несмотря на престиж бренда и необходимые условия функционирования, инвестор может изменить направление своей деятельности в сторону другогорегиона в случае, если посчитает отношение к его работе со стороны региона неуважительным или обнаружит иные препятствия.

Успех программы создания ОЭЗ в России напрямую зависит от того, в какой степени удастся в особых экономических зонах создать экономическую систему, максимально приближенную к идеальной — с четкими правилами игры, минимальными бюрократическими издержками и максимальной конкурентной средой, что сделало бы инвестиционный климат в зонах наиболее благоприятным. Это, в свою очередь, привлекло бы крупных инвесторов, что позволило бы повысить эффективность функционирования ОЭЗ. В результате страна и ее регионы укрепили свою экономическую безопасность.

В России опыт создания первых свободных экономических зон былотрицателен. К сожалению, он не дал ожидаемого эффекта ни в привлечении инвестиций, ни в качестве одного из инструментов развития депрессивных регионов РФ. М. В. Рубченко в своей статье свободные экономические зоны назвал «черными дырами», подчеркнув, что «свободные экономические зоны – это дефективный ребенок, обреченный на жалкое и бесславное существование»[2].

Причин такого резкого провала было несколько. Рассмотрим основные из них. Иностранные предприниматели обычно приглашаются в зону после того, как там создана необходимая инфраструктура. А капиталовложения в инфраструктуру составляют основную долю всех затрат, связанных с созданием и функционированием СЭЗ. Поэтому примерно 80% всех инвестиций в СЭЗ приходится на внутренние источники капиталовложений. В России

[1] Сайт Россия Сегодня [Электронный ресурс]. – Режим доступа: https://ria.ru/economy, дата обращения: 12.09.2018.

[2] Смородинская Н.В, Капустин А.Г. Свободные экономические зоны: мировой опыт и российские перспективы // Н.В. Смородинская, А.Г. Капустин. – С.-П., 2016. 4 с. (543 с.)

же многие надеются покрыть основные первоначальные затраты за счет иностранных источников, что зарубежным предпринимателям просто непонятно.

Вторая ошибка, допускаемая при организации СЭЗ, - совершенно необоснованный расчет на крупные прибыли уже после двух-трех лет их функционирования. С особой осторожностью следует подходить к созданию СЭЗ в восточных районах страны, где и сроки строительства длиннее, и затраты выше, и среднее качество продукции ниже.

Кроме того, планка продукции (50%), что должна была быть поставляема на экспорт, была существенно завышена, т.к. на тот момент продукция России, которую можно было бы отнести к высокотехнологичной, составляла 1,5% экспорта страны[1].

Попытки создания СЭЗ в границах целых областей и краев не могли увенчаться успехом. За дело взялись неграмотно, одержимые только одним желанием – получить иностранные инвестиции, или инвестиции из федерального бюджета, обеспечить себе льготы и привилегии за счет остальных регионов. Совершенно не учитывалось, что при этом целая область или край должны быть практически исключены из единого таможенного пространства России[2].

Еще одной серьезной причиной провала первых экономических зон России – это высокая степень коррупции.

Таким образом, слабыми сторонами особых экономических зон первого поколения в России можно отнести: увлечение гигантскими масштабами территории, грандиозность производственных планов и инвестиционных ожиданий, нечеткость механизма предоставления льгот предпринимателям, сложность в ряде случаев экологических проблем. Нельзя не отметить и стремление местной администрации ограничить свободу трансграничного перемещения товаров.

В частности, речь идет о Калининградской области, где через неделю после принятия федерального закона о создании зоны местная администрация «продавила» постановление правительства РФ о резком ограничении импорта большого перечня товаров на территорию области.

Одна из главных причин была в том, что многие аспекты деятельности этих зон и их резидентов не были четко отрегулированы в законодательстве. Результат этого известен: почти все зоны, по сути, были внутренними оффшорами, а их резиденты не вели экономической деятельности, направленной на развитие регионов, где была зарегистрирована та или иная особая экономическая зона.

Проведенная в 2015 году активистами народного фронта проверка 17 площадок, выделенных для ОЭЗ, опровергла данные отчетов.

Так, за 11 лет, с 2007 года, когда создали туристическо-рекреационную зону «В гостях у сказки» в Иркутской области, была разработана концепция и план развития ее за 119 млн. рублей. По факту – это пустая заболоченная местность, где до сегодняшнего дня никаких работ не производилось. Если говорить об эффекте, то это убыток в 119 миллионов. А если грубо подсчитать упущенную выгоду, то с банковским процентом за 11 лет убыток достигнет 226 миллионов.

Второй объект – технико-внедренческий кластер в Зеленограде. На выделенном участке земли построены 2 объекта на частные деньги за 1,5 миллиарда и за 100 миллионов рублей, не вступившие в строй из-за невыполненных обязательств государства и региона по обеспечению инфраструктурой и неподключением электроэнергии.

В Алтайском крае из четырех запланированных ОЭЗ реализуется только одна. Это «Озеро Алтай», на которое потрачен 1 миллиард рублей, так и не введенное в строй, не видевшее ни одного туриста. В отчетах отражено как введенное в строй[3].

---

[1] Андреев В.К. Правовое регулирование создания и деятельности особых экономических зон // Государство и право. 2016. №7. - 43-47 с.

[2] Архипов А.Ю., Черковец О.В. Внешнеэкономическая деятельность российских регионов // Ростов н/Д. Феникс, 2017. 103С. (192 с.)

[3] Сайт «Консультант плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru, дата обращения: 14.11.2018.

Торжественное открытие ОЭЗ «Советская гавань» в Хабаровском крае состоялось 6 лет назад. С тех пор там ни один предприниматель не получил статуса резидента из-за долгих, по 2 года согласований. Из выделенных 3-х миллиардов освоено было 44,7 миллиона[1].

В Ульяновской области на ОЭЗ из пяти заявленных резидентов стройку ведут только двое. АО «ОЭЗ» отчиталось о наличии там таможенного пункта еще в 2013 году. На самом деле ни один объект там не введен в эксплуатацию. На него выделено из бюджета 7 миллиардов рублей, освоено 1 миллиард. На что он освоен представителям Народного фронта так и не удалось увидеть.

АО «ОЭЗ» разработало (погодовому отчету) 2 концепции развития ОЭЗ, в том числе в Иркутской области за 250 миллионов рублей, которые являются с их слов секретными и их никто не видел. Тогда как стратегия развития и долгосрочная программа развития АО ОЭЗ до сих пор не разработана. Система ключевых показателей эффективности в АО «ОЭЗ» в настоящее время не утверждена[2].

Одновременно с этим, АО «ОЭЗ» имеет уставный капитал (по закону это взносы учредителей, предназначенные на вклад в инфраструктуру ОЭЗ) в размере 121,6 миллиардов рублей и фонд оплаты труда в размере 800 миллионов рублей в год. Из 121, 6 миллиардов рублей направлено на финансирование строительства объектов инфраструктуры 45,7 миллиардов рублей. Остальные деньги АО держит на депозитах в банках, получая прибыль и расходуя ее по своему усмотрению.

АО «ОЭЗ» является посредником между Департаментом особых экономических зон в Министерстве экономического развития РФ и регионами, в которых находятся ОЭЗ. Департамент состоит из директора, 4 заместителей и 8 отделов, с сотнями специалистов и соответствующим бюджетом.

Причем функции АО «СЭЗ» (кроме коммерческих услуг) дублируются с функциями Департамента (стр. 22 Годового отчета АО «СЭЗ» и данные из сайта Департамента). При этом, плановые документы по созданию и функционированию особых зон обе структуры готовили плохо, затягивая процесс на годы. Объекты инфраструктуры, которые так ждут инвесторы, строились медленно. Причем сроки сдачи постоянно срывались, что в свою очередь вело, к удорожанию работ.

В итоге из 758 запланированных объектов сданы в эксплуатацию 526. Если по плану общая стоимость строительства объектов инфраструктуры оценивается в 334,2 миллиарда рублей, то по факту это 635 миллионов рублей.

В 2016 году Президент поручил Генпрокуратуре, Счетной палате России, Федеральной налоговой службе и Росфинмониторингу проверить эффективность расходования компанией «Особые экономические зоны» бюджетных средств. Выводы российских аудиторов следующие: «Процесс создания и управления ОЭЗ характеризуется формализмом, безответственностью и безнаказанностью, отсутствием исполнительной дисциплины и спроса за принятые решения и их последствия. Реальный экономический эффект от особых экономических зон не достигнут», (выступление С. Агапцова на заседании коллегии СП РФ 04.04.2016)[3].

Председатель Счетной палаты Т. Голикова обосновала это цифрами: – «На территории ОЭЗ за 10 лет создано 18 177 рабочих мест. Давайте соотнесем 121,9 млрд, которые вложили из федерального бюджета, 185,9 млрд руб. – вместе с субъектами, и 18 177 рабочих мест: разделите, сколько стоит одно рабочее место за 10 лет.

Таким образом, на создание одного рабочего места было потрачено 10,2 миллиона рублей. Этой суммы хватит, чтобы человек 25 лет получал среднюю зарплату по стране»[4].

По результатам расчетов Голикова предложила уменьшить бюджетное финансирование акционерного общества «Особые экономические зоны» на 3,1 миллиарда рублей, так как на

---

[1] Там же.

[2] Там же.

[3] Сайт «bankir.ru» [Электронный ресурс]. – Режим доступа: http://bankir.ru, дата обращения: 14.11.2018.

[4] Сайт Правительства России [Электронный ресурс]. – Режим доступа: http://government.ru, дата обращения: 10.11.2018

счетах этой компании на 1 января 2016 года образовались остатки неиспользованных бюджетных средств в размере 3,5 миллиарда рублей, на счетах дочерних обществ проекта осталось 21,3 миллиарда рублей. При этом у компании отсутствуют утвержденные основные плановые документы по созданию особой экономической зоны промышленно-производственного типа во Владивостоке. В выступлении пресс-секретаря президента РФ Дмитрия Пескова прозвучало, что практика ОЭЗ оказалась «с нулевым КПД».

Кроме того, такие огромные средства явились приманкой для нечистых на руку распорядителей средствами. Так, возбуждено 5 уголовных дел о хищении 509 миллионов рублей, предназначенных на развитие инфраструктуры Липецкой области, много вопросов у Генпрокуратуры к ОЭЗ в Приморском и Хабаровском краях, в Мурманской области и к ОЭЗ туристического кластера Северного Кавказа.

В апрельском отчете Счетная палата заявила о необходимости доработать механизм создания, развития и управления ОЭЗ, включая требования к целесообразности создания, доходности, рентабельности и срокам окупаемости.

Библиографический список

1. Сайт Россия. Особые экономические зоны [Электронный ресурс]. – Режим доступа: http://www.russez.ru
2. Сайт Русская планета [Электронный ресурс]. – Режим доступа: http://rusplt.ru/sub/economy
3. Сайт Россия Сегодня [Электронный ресурс]. – Режим доступа: https://ria.ru/economy
4. Смородинская, Н.В, Капустин, А.Г. Свободные экономические зоны: мировой опыт и российские перспективы // Н.В. Смородинская, А.Г. Капустин. – С.-П., 2016. – 543 с.
5. Андреев, В.К. Правовое регулирование создания и деятельности особых экономических зон // Государство и право. 2016. №7. - 43-47 с.
6. Архипов, А.Ю., Черковец, О.В. Внешнеэкономическая деятельность российских регионов // Ростов н/Д. Феникс, 2017. – 192 с.
7. Сайт «Консультант плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru
8. Сайт «bankir.ru» [Электронный ресурс]. – Режим доступа: http://bankir.ru
9. Сайт Правительства России[Электронный ресурс]. – Режим доступа: http://government.ru

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СФЕРЕ НАЛОГООБЛОЖЕНИЯ

Абдалова А.А., студент
Научный руководитель: Шехтман А.Ю., ст. преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

С развитием экономики в России возникла необходимость реформирования и оптимизации налогового законодательства, стимулирования или сдерживания различных отраслей и сфер деятельности экономики, а также государственного регулирования финансовой деятельности хозяйствующих субъектов.

Налоги и налоговая политика являются важнейшим элементом системы обеспечения экономической безопасности. Значение налоговой составляющей экономической безопасности многократно возрастает по мере перехода к экономике, базирующейся на рыночных принципах и механизмах хозяйствования. Это актуализирует проблему налоговой безопасности в системе экономической безопасности, а также выдвигает в качестве одной из приоритетных задач в сфере обеспечения национальной экономической безопасности разработку комплекса мер, направленных на противодействие и нейтрализацию угроз. В связи с этим

определяется актуальность темы статьи.

Цель данной работы выявить проблемы обеспечения безопасности в сфере налогообложения. Исходя, из поставленной цели можно обозначить задачи нашей работы:

- дать понятие экономической безопасности в сфере налогообложения;
- определить основные проблемы в рамках данного вопроса;
- предложить мероприятия по устранению угроз экономической безопасности налогообложения.

На сегодняшний день говорить об обеспечении налоговой безопасности в Российской Федерации определенно трудно, та как в России прочно укрепились такие понятия как «двойная бухгалтерия», «зарплата в конверте», «теневая экономика». Следовательно, несовершенство налоговой системы препятствует реализации налогами своих основных функций. Одной из них является фискальная функция. Ее суть заключается в финансовом обеспечении деятельности государства. Таким образом, следует сказать, что налоговая система является одновременно ресурсом и инструментом обеспечения экономической безопасности, и фактором возникновения угроз.

В раках данной статьи нам необходимо выделить основные проблемы обеспечения экономической безопасности налогообложения.

В первую очередь это уклонение от уплаты налогов. В Российской Федерации эти показатели также слишком высоки для экономически безопасного государства. Способы уклонения от налогов на сегодняшний день достаточно разнообразны, поэтому их можно объединить в следующие группы:

1. полное или частичное искажение информации в бухгалтерской финансовой отчетности;
2. проведение операций с наличностью без соответствующей фиксации в учетных документах;
3. необоснованное отнесение различных затрат на издержки производства;
4. умышленное занижение или завышение экономических показателей;
5. занижение объемов приобретенной или реализованной продукции;
6. маскировка объекта налогообложения (подмена, лжеэкспорт);
7. махинации с помощью фирм-однодневок или посреднических аффилированных лиц [9].

Причины, побуждающие физических и юридических лиц уклонятся от уплаты налогов, могут быть самыми разнообразными, начиная с безвыходности вследствие финансового положения и платежеспособности бизнеса и населения, наличия «пробелов» в налоговом законодательстве и заканчивая психологическими аспектами поведения людей [4].

Вместе с тем, весьма важно отметить о налоговой культуре общества, которая также предопределяет степень уплаты налогов в бюджет. По данным опроса, проведенного Фондом «Общественное мнение», 69% опрошенных респондентов считают, что уплачивать налоги нужно всегда, независимо от жизненных обстоятельств. Данный показатель, с учетом того, что только 33% опрошенных считаю уплату налогов своим долгом, а 52% делают это из-за страха, может явиться доказательством довольно низкого уровня налоговой культуры и налоговой морали в Российской Федерации.

Так же важно выделить проблемы налогообложения в другом ракурсе, с точки зрения не обеспечения экономической безопасности всего государства, а со стороны хозяйствующих субъектов. Одной из основных проблем выступает конфликтность налоговых правоотношений, которая заключается в том, что один участников – налоговый орган – правомочен применить к противной стороне (налогоплательщику) меры принуждения, что обуславливает объективную необходимость защиты налогоплательщиков от неправомерных действий налоговых органов в рамках обеспечения экономической безопасности. Последние в свою очередь руководствуются задачей по наполнению бюджетной системы и поэтому непосредственно заинтересованы в применении к налогоплательщику штрафных финансовых санкций. В результате деятельность налоговых органов по контролю за соблюдением налогового законодательства остается недостаточно эффективной. В связи с этим необходимо, чтобы права и обязанности обеих сторон налоговых правоотношений были не просто продекларированы, а имели четкие механизмы реализа-

ции и были снабжены указаниями на правовые последствия их нарушения и неисполнения. В результате проведенного исследования, мы выяснили, что рассмотренная проблема выше, не является исчерпывающей. На орган власти по обеспечению налогообложения возлагается обязанность информировать налогоплательщика об изменениях в налоговом законодательстве или о тех налогах, которые он должен уплачивать, то необходимо указать, какие последствия наступят, в том случае если налогоплательщик неправильно подсчитает налоговые суммы или не уплатит вовремя тот или иной налог по вине налогового органа.

Кроме изложенного, отмечается и факт отсутствия стабильности в области налогового законодательства России, это обуславливается тем, что сегодня достаточно часто вносятся различного рода поправки и изменения, которые, при этом, имеют обратную силу, также нередко ликвидируются ранее введённые привилегии, что, так или иначе, создаёт дополнительный источник риска для инвесторов.

Государство должно гарантировать соблюдение стабильности налогов и правил их взимания в течение значительного периода времени. Налоги не должны пересматриваться чаще, чем раз в несколько лет. При этом обо всех планируемых изменениях налогоплательщиков необходимо извещать до периода их действия, а не ставить перед уже свершившимся фактом.

При этом, проблемный аспект видится и в наличии рисков хозяйствующих субъектов, которая выражается посредством проявления возможности или же угрозы финансовых либо иных потерь, которые связанны с формированием, а равно и расходованием фондов денежных средств государства.

Необходимо осознавать и то, что предприятие, при реализации своей деятельности, может столкнуться с негативным воздействием налоговых факторов, например до взыскание налогов, начисление пеней или же наложение штрафа. Последствием такого воздействия может стать экономический или финансовый убыток. В связи с чем, видится значимой разработка мер, направленных на искоренение либо существенное сокращение налоговых рисков, повышение налоговой безопасности.

Видится, что достаточно существенным на сегодня является и вопрос, касающийся повышения эффективности именно налогового контроля. Отмечается отсутствие законодательной регламентации реализации такого контроля, а именно продолжительности (сроков) проверок, пояснений форм таковых, а равно и процедур участия непосредственно налогоплательщиков при рассмотрении актов данных проверок.

Предполагается, что разрешить сложившуюся ситуацию возможно при принятии нижеследующих мер:

1) посредством создания системы отбора налогоплательщиков, в отношении которых вероятность обнаружения нарушений высока, что позволило бы выстраивать процесс проведения контрольных проверок, что, в свою очередь, позволило бы выбрать наиболее оптимальное направление использования ограниченных кадровых и материальных ресурсов налоговой инспекции, достигая значительной результативности проверок, минимизируя при этом затраты усилий, а также и средств;

2) применением наиболее продуктивных форм, методов, приемов налоговых проверок, которые базируются на подготовленной налоговым органом (ведомством) стандартной единой комплексной процедуре реализации указанных проверок, в том числе с учетом законодательной базы, позволяющей налоговым органам осуществлять действия, сущность которых заключается в правовом воздействии на недобросовестных налогоплательщиков;

3) посредством применения системы оценки работы налоговых инспекторов, что, как видится, будет способствовать объективному учету результатов соответствующей контрольной деятельности каждого из таковых.

Относительно, косвенного налогообложения, то сфере проведения налоговой политики присущ, как правило, фискальный характер, который, при этом затрудняет межотраслевой небанковский «перелив» капитала, а также становится причиной возникновения барьеров на пути развития финансовых операций.

Так, по мнению И.А. Пушкаренко, тенденция по изъятию любых денежных средств, кото-

рые, в свою очередь, поступают на счет того или иного предприятия, не может считаться в полной мере справедливой и обоснованной. В связи с чем, наиболее целесообразным решением сложившейся ситуации видится ужесточение штрафов по несвоевременным расчетам и сокрытой величине на учётную ставку процента Центрального банка Российской Федерации.

В отношении же организаций и предприятий видится необходимым обратить особое внимание именно на амортизационную политику, ввиду того, что последняя имеет связь с налогообложением таких субъектов налоговых правоотношений, определяя при этом уровни налогооблагаемых баз налогов не только на имущество, но и прибыль. В связи с чем, следует предположить, что решение проблем в указанной области, касаемо амортизационной политики, будет основываться на успешном практическом участии оценщиков. Такая благоприятная тенденция может быть достигнута посредством двух аспектов: 1) более полной необходимой информационной базой по управлению амортизационным фондом; 2) опытом, профессионализмом исполнителей работ по оптимизации данного направления в политике.

Таким образом, подводя итог вышеизложенного, следует еще раз отметить, что сфера налогообложения сегодня, несмотря на периодическое совершенствование, отражает и ряд проблемных аспектов, что позволяет своевременно выявлять недочеты действующей системы, предпринимая меры по их устранению.

Библиографический список

1. Балынин, И.В. Рейтинговая оценка субъектов Российской Федерации по уровню риска несбалансированности региональных бюджетов (на основе разработанной модели) // РИСК: Ресурсы, информация, снабжение, конкуренция. 2014. № 3. С. 104-109.

2. Балынин, И.В. Формирование социально ориентированной бюджетной политики в Российской Федерации на региональном уровне // Финансы и кредит. 2015. № 30. С. 48-59.

3. Дивина, Л.Э. Налоговая составляющая экономической безопасности Российской Федерации // Российское предпринимательство. 2014. №8 (254) - с. 39-45.

4. Жарова, Е.Н., Желтова, М.Ф. Уклонение от уплаты налогов: причины, масштабы проявления и методы противодействия // Молодой ученый. 2013. №6 - с. 336-339.

5. Костюков, А.Н., Маслов, К.В. Правовые аспекты обеспечения налоговой безопасности государства // Вестник Омского университета. Серия «Право». 2015. №4 (45) - с. 117-121.

6. Юнева, Е.А. Институциональные ловушки современной российской экономики как фактор теневизации // Educatio. 2015. №3-10 (2) - с. 91-93.

7. The Global Competitiveness Report [Электронный ресурс]. - Режим доступа: http://reports.weforum. org. - (Дата обращения: 8.11.2018).

8. Tax Justice Network [Электронный ресурс]. - Режим доступа: http://www.taxjustice.net. - (Дата обращения: 29.11.2018).

СТРАТЕГИЯ РАЗВИТИЯ КАК ПОРТФЕЛЬ ПРОЕКТОВ БЕЗОПАСНОГО РАЗВИТИЯ ЭКОНОМИЧЕСКИХ СИСТЕМ

Афоничкин А.И., д. э. н., профессор
Самарский национальный исследовательский университет имени академика С.П. Королева
г. Самара
Волжский университет имени В.Н. Татищева
г. Тольятти
Сыропятова С.Б., к. ю. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

Роль регионов в настоящее время оказывает очень сильное воздействие на преобразование форм и инструментов конкуренции, приводя, по сути, к формированию особой ее формы – межрегиональной конкуренции, которая, в свою очередь, предъявляет новые требования к конкурентоспособности региона, как полноправного субъекта глобального рынка.

Конкурентоспособность является одной из основных экономических категорий в рыночных отношениях, которая формируется на уровнях товара, предприятия, отрасли, региона, страны и в общем виде выражает способность выдерживать соперничество с другими аналогами.

Состояние привлекательности города - это среда, в которой протекают процессы непрерывного формирования и использования инвестиционных ресурсов с целью достижения стратегических и оперативных целей деятельности субъектов города. Привлекательность формируется под воздействием комплекса взаимосвязанных законодательно-нормативных, организационно-экономических, социально-политических и других факторов, определяющих условия инвестиционной деятельности.

Конкурентоспособность и привлекательность формируется рядом экономических, социальных и природно-географических факторов, которые, в совокупности составляют потенциал города. Рассмотрим более подробно потенциальные точки роста конкурентоспособности и привлекательности – трудовой, потребительский, производственный, инфраструктурный и финансовый потенциал г.о. Тольятти.

Теория межрегиональной конкуренции, основана, с одной стороны, на базовом методологическом аппарате классической и неоклассической теорий, с другой стороны - на теориях, изучающих влияние «фактора пространства» на экономическое развитие региона. существуют различные трактовки понятия «конкурентоспособность региона», однако, отсутствие единого подхода к формированию определения затрудняет понимание её объективной сущности.

В общем смысле под конкурентоспособностью региона понимают такую модель экономического пространства, которая способна обеспечить высокий уровень жизни населения и возможность реализовать имеющийся в регионе экономический потенциал (финансовый, производственный, трудовой, инновационный, ресурсно-сырьевой.

Конкурентоспособность региона определяется многими факторами, состояние и изменение которых определяется его предшествующим развитием, состоянием инфраструктуры, условиями для жизни населения, человеческим потенциалом, обстановкой для ведения бизнеса, усилиями власти по улучшению социально-экономического положения в регионе и т.д.

На первое место в качестве движущей силы региональной конкурентоспособности ставят следующие факторы – параметры конкурентоспособности и привлекательности.

Согласно исследованиям Рейтингового агентства «Эксперт», Самарская область в 2015-2017 гг. продемонстрировала рост инвестиционной привлекательности, войдя в пятерку лучших регионов страны по показателям динамики инвестиционного потенциала и инвестиционного риска.

В настоящее время Самарская область вошла в «Средний потенциал - умеренный риск», показав 5-й результат после Башкортостана, Татарстана, Пермского края и Нижегородской области.

Таблица 1 - Параметры конкурентоспособности и привлекательности региона

Факторы	**Параметры**
Географическое положение	Выгодное
Обеспеченность природными ресурсами и их доступность	Уровень обеспеченности природными ресурсами высокий и ресурсы доступны
Состояние окружающей среды	Экологическая обстановка нормальная
Структурное разнообразие экономики	Структура экономики адекватна требованиям рынка
Состояние и развитие инфраструктуры рынка	Системы инфраструктуры работают быстро и надежно
Развитие культуры и образования населения	Уровень образования и квалификации населения высокий и существуют возможности для обучения нужным профессиям
Социально-политическая стабильность	Социально-политический климат безопасный

Продолжение таблицы 1

Экономическая стабильность	Уровень производственных затрат, которые контролируются властями, низок; существует доступ к инвестиционному капиталу и кредитным ресурсам; оказывается содействие внешнеэкономической деятельности со стороны администрации
Взаимодействие органов управления с предприятиями	Взаимодействие администрации города и предприятий города взаимовыгодное и прозрачное
Информационное и коммуникационное поле	Уровень оснащенности передовыми технологиями высокий
Нормативно-правовое поле	Состояние хозяйственного законодательства и регулирования не ограничивают развитие производства
Система льгот инвесторам	Налоговая система приемлема и стабильна

По инвестиционному риску Самарская область заняла в данном рейтинге 17-е место, улучшив прежний показатель на 21 пункт, что позволило войти в пятерку лучших по динамике инвестиционного риска и занять в ней 4-е место после Ставропольского, Алтайского и Хабаровского краев. Среди субъектов ПФО по показателю инвестиционного риска область на 3-ем месте после Татарстана и Башкортостана.

Основными факторами, нивелирующими риски инвесторов в регионе, стали финансовый (13-е место) и социальный (21-е место). Умелая финансовая политика наряду с социальной стабильностью становятся, по мнению агентства, одним из решающих позитивных факторов привлечения инвесторов.

Сравнивая преимущества и барьеры, можно сделать вывод, что унаследованные факторы развития и современная ситуация в Самарской области более благоприятны по сравнению с подавляющим большинством российских регионов.

Основными преимуществами являются:

−трансграничное географическое положение, высокий транспортный потенциал;

−наличие уникального природного комплекса – Самарская Лука;

−наличие мощной двухцентровой Самарско-Тольяттинской агломерации, высокая урбанизированность региона;

−высокий уровень экономической активности населения, образованности и квалифицированности рабочей силы;

−сравнительно высокий уровень жизни, значительная миграционная привлекательность региона;

−наличие ресурсов углеводородного сырья, развитая инфраструктура нефтедобывающей отрасли;

−многоотраслевая структура экономики региона и ведущей отрасли –промышленности;

−значительная концентрация на территории области крупных российских и зарубежных компаний;

−высокий инновационный потенциал, развитая инфраструктура инновационной деятельности;

−высокий уровень развития телекоммуникаций и связи;

−полиэтничность и мультикультурность региона, устойчивый уровень толерантности в национально-культурных и межконфессиональных отношениях;

−активное становление гражданского общества;

−устойчивый имидж открытого и реформаторского региона, сравнительно высокий уровень развития рыночных институтов и качества регионального менеджмента, наличие постоянного и конструктивного диалога власти, бизнеса и гражданского общества

Проведенный анализ определил возможные узкие места и ведущие звенья в развитии конкурентоспособности и привлекательности Самарской области.

Основным барьером является инфраструктурная составляющая. Финансовый потенциал Тольятти характеризуется как стабильный. Сохраняются приоритетные направления на дальнейшее развитие таких социально-значимых для городского округа отраслей муниципального хозяйства, как жилищное строительство, образование, здравоохранение энергообеспечение, коммунальное строительство и спорт, что, несомненно, повысит уровень кадрового потенциала

Анализ региональной практики позволил обосновать три подхода к повышению конкурентоспособности региона – подход на основе выявления и углубления ключевой компетенции, подход на основе использования внешних возможностей и комбинированный подход. Выбор конкретного подхода определяется соответствием социально-экономических и структурных особенностей региона набору критериев, сформулированных в рамках каждого из них.

Таблица 2 - Подходы к повышению конкурентоспособности региона

Характеристики	**1. Подход на основе выявления и углубления ключевой компетенции**	**2. Подход на основе использования внешних возможностей**	**3. Комбинированный подход**
Аналитическая основа	Анализ внутренней среды с целью выявления ключевой компетенции региона	Анализ внешней среды с выявлением возможностей и перспективных ниш	Структурный анализ возможностей углубления традиционной специализации и диверсификации
Суть подхода	Формирование окружения (инфраструктуры, производств), поддерживающего ключевую компетенцию	Создание и развитие в регионе базовых условий, позволяющих использовать внешние возможности	Концентрация цепочек создания стоимости в специализирующих секторах и развитие поддерживающих отраслей
Приоритетные конкурентные стратегии	Стратегия специализации и экспансии на внешние рынки	Стратегия диверсификации и привлечение внешних клиентов	Стратегия специализации и качественного роста в сочетании со стратегией диверсификации
Результат	Ярко выраженная узкая специализация экономики с комплексом поддерживающих видов деятельности	Широкая специализация экономики региона, обусловленная высоким уровнем развития инфраструктуры	Повышение эффективности секторов традиционной специализации региона с внутриотраслевой диверсификацией

Применительно к Самарской области предлагаем комбинированный подход, который представляет собой соединение первых двух подходов и характеризуется системным воздействием на экономику региона. С одной стороны, он направлен на углубление ключевой компетенции региона, наращивание конкурентных преимуществ.

С другой стороны, он направлен на создание базовых условий для использования возможностей развития, предоставляемых внешней средой, возможностей «встраивания» своих хозяйствующих субъектов через интенсивное развитие технологической специализации.

Реализация данного подхода предполагает повышение конкурентоспособности предприятий, компаний и продуктов, относящихся к специализирующим секторам экономики региона и, одновременно, развитие поддерживающих секторов как основы для дальнейшей диверсификации экономики.

ПОДХОДЫ К СОВЕРШЕНСТВОВАНИЮ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ПОТРЕБИТЕЛЬСКОГО КРЕДИТОВАНИЯ

Вайтонис Т., студент
Научный руководитель: Шехтман А.Ю., ст. преподаватель
Волжский университет имени В.Н. Татищева
г. Тольятти

Сфера потребительского кредитования, весьма подвержена микро и макро факторам, которые негативно влияют на экономическую безопасность кредитной организации. Социально-экономическое развитие страны характеризуется совокупностью макроэкономических параметров, взаимозависимость которых определяет динамику этого процесса. Потребительский кредит занимает определенное место в совокупности данных параметров. Необходимо исследовать влияние потребительского кредита на основные макроэкономические показатели с учетом тенденций развития, характерных для России, в целях определения направлений обеспечения экономической безопасности. Имеется ряд макроэкономических показателей, характеризующих экономическое развитие страны, которые, с точки зрения автора, зависят от развития потребительского кредитования

Актуальность темы обусловлена в первую очередь, тем, что в настоящее время одним из динамично развивающихся направлений банковской деятельности является потребительское кредитование. Цель данной статьи: выявить тенденции и проблемы обеспечения экономико-правовой безопасности кредитной организации в сфере потребительского кредитования населения. Исходя, из поставленной цели можно обозначить задачи нашей работы:

- дать понятие экономической безопасности в сфере потребительского кредитования;
- определить основные аспекты в рамках данного вопроса;
- предложить мероприятия по устранению угроз экономической безопасности.

Потребительское кредитование способствует повышению уровня потребления и позволяет быстрее удовлетворять разнообразные потребности населения. В современной экономике главными кредиторами являются коммерческие банки. Банковская форма кредита - наиболее распространенная форма, поскольку именно банки чаще всего предоставляют свои ссуды субъектам, нуждающимся во временной финансовой помощи. По объему ссуда при банковской форме кредита значительно больше ссуд, выдаваемых при каждой из других его форм. Банк является особым субъектом, основополагающим занятием которого чаще всего становится кредитное дело, он организует многократное круговращение денежных средств на возвратной основе. Банк ссужает не просто денежные средства, а деньги как капитал. Это означает, что заемщик должен так использовать полученные в банке средства, чтобы не только возвратить их кредитору, но и получить прибыль, достаточную, по крайней мере, для того, чтобы уплатить ссудный процент.

В соответствии с российским законодательством, кредитная организация - это юридическое лицо, которое для извлечения прибыли как основной цели своей деятельности на основании специального разрешения (лицензии) Центрального банка Российской Федерации (Банка России) имеет право осуществлять банковские операции, предусмотренные Федеральным законом «О банках и банковской деятельности». Виды кредитных организаций (в соответствии с законом РФ «О банках и банковской деятельности»):

1. Банк - кредитная организация, которая имеет исключительное право осуществлять в совокупности, следующие банковские операции: привлечение во вклады денежных средств физических и юридических лиц, размещение указанных средств от своего имени и за свой счёт на условиях возвратности, платности, срочности, открытие и ведение банковских счетов физических и юридических лиц;

2. Небанковская кредитная организация - кредитная организация, имеющая право осуществлять отдельные банковские операции, предусмотренные ФЗ «О банках и банковской деятельности». Допустимые сочетания банковских операций для небанковских кредитных

организаций устанавливаются ЦБР;

3. Иностранный банк - банк, признанный таковым по законодательству иностранного государства, на территории которого он зарегистрирован.

В настоящее время самым распространенным видом кредитования является потребительское. Так по данным статистики услугами банков воспользовались около 30–35% населения. Вследствие этого государство должно обеспечивать информационную безопасность в сфере потребительского кредита (займа) [1].

Сущность потребительского кредита заключается в предоставлении денег либо товаров, услуг в долг с рассрочкой платежа по целевому назначению на условиях возвратности и срочности. Главная его роль в перераспределении капитала между отраслями народного хозяйства, стимулируя эффективность труда, ускорения сбыта товаров.

Процесс потребительского кредитования в наиболее полном виде включает несколько этапов. Прежде всего, кредитный работник ведет переговоры с клиентом с целью выяснения: кредитоспособности клиента в юридическом смысле, т.е. является заемщик дееспособным в целях вступления в кредитные отношения; кредитоспособности клиента с экономической точки зрения, т.е. имеет ли он экономические предпосылки (доходы, имущество), необходимые для полного и своевременного выполнения условий кредитного договора с точки зрения возврата долга, уплаты процентов; характера обеспечения кредита.

Анализ кредитоспособности клиента предшествует заключению с ним кредитного договора и позволяет выявить факторы риска, способные привести к непогашению выданной банком ссуды в обусловленный срок, и оценить вероятность своевременного возврата ссуды. Определение кредитоспособности заемщика является неотъемлемой частью работы банка по определению возможности выдачи ссуды.

Оценка кредитоспособности клиента проводится в кредитном отделе банка на основе информации, характеризующей способность клиента получать доход, достаточный для своевременного погашения ссуды, служить обеспечением выданной ссуды и т.д. Кроме того, банковский работник должен анализировать рыночную конъюнктуру, тенденции ее изменения, риски, которые испытывают банк и его клиент и прочие факторы. Источниками информации об индивидуальном заемщике могут быть сведения с места работы, места жительства, налоговых органов и т.д.

Для выяснения кредитоспособности заемщика кредитный работник анализирует доходы и расходы клиента. Доходы, как правило, определяются по трем направлениям: доходы от заработной платы, сбережений и капитальных вложений, прочие доходы. К основным статьям расходов заемщика относятся: уплата налогов, алименты, платежи по ранее полученным и непогашенным ссудам, коммунальные платежи и т.д. Подтверждение размеров доходов и расходов возлагается на клиента, который предъявляет в банк необходимые документы: паспорт; справку с места работы о среднемесячной заработной плате и удержаний из нее либо декларацию о доходах и расходах, подтвержденную налоговой инспекцией; свидетельство о постановке на учет в налоговой инспекции (ИНН) и пенсионном фонде; заполненные анкеты по установленной банком форме; другие документы в случае необходимости. Банк проводит анализ платежеспособности заемщика и его поручителя (при необходимости). При этом методы анализа одинаковы. Таким образом, при положительной оценке кредитоспособности клиента банк и заемщик приступают к согласованию условий кредитного договора в части объема, срока кредита, способов погашения основного долга и процентов.

Обеспечение экономической безопасности - это гарантия независимости субъекта экономической деятельности, условие стабильности и эффективного функционирования, достижения успеха. Обеспечение экономической безопасности принадлежит к числу важнейших приоритетов коммерческих структур

Основными задачами экономической безопасности в сфере потребительского кредитования являются:

обеспечение пропорционального и непрерывного экономического роста;

–формирование эффективной структуры;

–обеспечение социальной защиты;

–поддержание устойчивости организации и т.п.

Данные задачи определяют стратегию экономической безопасности как формирование и обоснование стратегических приоритетов, средств и механизмов решения проблем.

Экономическая безопасность в сфере потребительского кредитования населения основывается на том, насколько эффективно службам данной организации удается предотвращать угрозы и устранять ущербы от негативных воздействий на различные аспекты экономической безопасности организации. Под угрозой понимают совокупность условий, процессов, факторов, которые препятствуют реализации экономических интересов субъектов хозяйственной деятельности или создают для них опасность.

Исходя из вышеизложенного, мы можем сделать вывод, что экономическая безопасность кредитной организации в сфере потребительского кредитования - это состояние кредитной организации при котором кредитная организация достигает максимальную прибыль за счет оказания услуг по потребительскому кредитованию населения с минимизацией рисков.

Библиографический список

1. Боннер, Е.А. Банковское кредитование / Е.А. Боннер. - М.: Городец, 2016. - 160 с.

2. Брейли, Р. Принципы корпоративных финансов / Р. Брейли, С. Майерс. - М.: Олимп-Бизнес, 2017. - 840 с.

3. Гусев, А. Ипотечное жилищное кредитование. Жилье взаймы / А. Гусев. - М.: Феникс, 2017. - 690 с.

4. Бланк, И.А. Управление финансовыми рисками. - М.: Ника-Центр, 2016. – 448 с.

УПРАВЛЕНИЕ ПРОЦЕССОМ ВНЕДРЕНИЯ ТРЕБОВАНИЙ ГОСТ Р 57628-2017 В ДЕЯТЕЛЬНОСТЬ ПРОИЗВОДСТВЕННЫХ СТРУКТУР ПРИ РАЗРАБОТКЕ ПРОФИЛЕЙ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глухова Л.В., д. э. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти

Аннотация. *Построение профилей зашиты информационной безопасности является сегодня для любой бизнес-структуры обязательным атрибутом, направленным на ее эффективное функционирование. В статье показана интерпретация требований существующих стандартов к их содержанию.*

Рекомендовано для ознакомления и изучения топ-менеджменту промышленных предприятий.

Ключевые слова: *требования ГОСТ, менеджмент информационной безопасности, профиль защиты, требования к специалистам, занимающимся построением профилей защиты*

Стандартизация требований к функциональным обязанностям сегодня является той панацеей, которая влияет на снижение уровня риска деятельности бизнес-структур в сложных экономических условиях.

Анализируемый и изучаемый в статье нормативный документ (ГОСТ Р 57628-2017) представляет собой методику, опираясь на требования которой, возможно достижение целевых показателей, а именно - построение профиля защиты информационной безопасности для бизнес-структур. Будем в дальнейшем под бизнес-структурой понимать производственную структуру, имеющую потребность в обмене информационными потоками через сетевые коммуникации.

В период развития цифровых и информационных технологий на одно из первых мест

выносится проблема интеллектуализации знаний и формирования базы личностных показателей умений и навыков, позволяющих приобретать дальнейший опыт в направлении поиска и блокировки уязвимостей, возможных отказов и рисков потери важных информационных активов от несанкционированного доступа.

К сожалению, как показали результаты неоднократно выполняемого анализа результативности применения требований стандартов к процессам деятельности производственных структур, в частности, к процессам защиты информационных и других активов показал, что практическое использование требований стандартизации явно недостаточно. В связи с чем в статье рассматриваются особенности разработки профилей защиты информации в условиях производственной деятельности.

Обзор предпосылок к появлению рассматриваемого в статье нормативного документа, показал, что его появление закономерно. Только за последние несколько лет появились требования стандартов к формированию терминологической базы основных понятий, имеющих прямое отношение к построению компетенций, содержащих набор знаний, умений и навыков в предметной области управления процессами защиты информационной безопасности.

В таблице 1 отражены составляющие начального уровня базы знаний, которая должна быть сформирована на этапе изучения методики, описанной в анализируемом ГОСТ (ГОСТ Р 57628-2017) [1, с. 1-3].

Таблица 1 - Предпосылки к изучению требований по построению профиля защиты информационной безопасности на предприятии

Нормативный документ	Основное содержание извлекаемых знаний	Приобретаемые навыки и опыт деятельности
ГОСТ 15408.1-2012	База понятий, используемых при оценке информационной безопасности; операционный менеджмент по доработке требований к информационной безопасности для конкретного пользователя; терминологический словарь в области уровней доверия	Методика формирования профиля защиты по информационной безопасности (ПЗИБ). Методика формирования задания по безопасности (ЗЗИБ). Умение выстраивать причинно-следственные связи для оценки соответствия между целями, проблемой и требованиями безопасности.
ГОСТ 15408.2-2013	Классовая структуризация требований к функциональной обеспеченности информационной безопасности на предприятии. Состав и структура функциональных компонентов в разрезе классов. Понятие аудита информационной безопасности в разрезе этапов и стадий проведения	Методика построения требований к функциональным компонентам информационной безопасности. Методика определения ресурсов обеспечения ИБ. Методика определения доступа к объектам оценки (ОО). Первичные навыки построения доверительного маршрута.
ГОСТ 15408.3-2012	Базовые понятия доверия в сфере информационной безопасности. Оценочные уровни доверия.	Выбор компонентов доверия. Методики формирования и оценки уровней доверия, предусматривающих верификацию и тестирование (в разрезе различных классов).

На рисунке 1 отражены результаты проведенного опроса выпускников по направлению "организация защиты информации" в 2017 г, которые отразили недостаточный уровень сформированности компетенции построения профилей защиты информации.

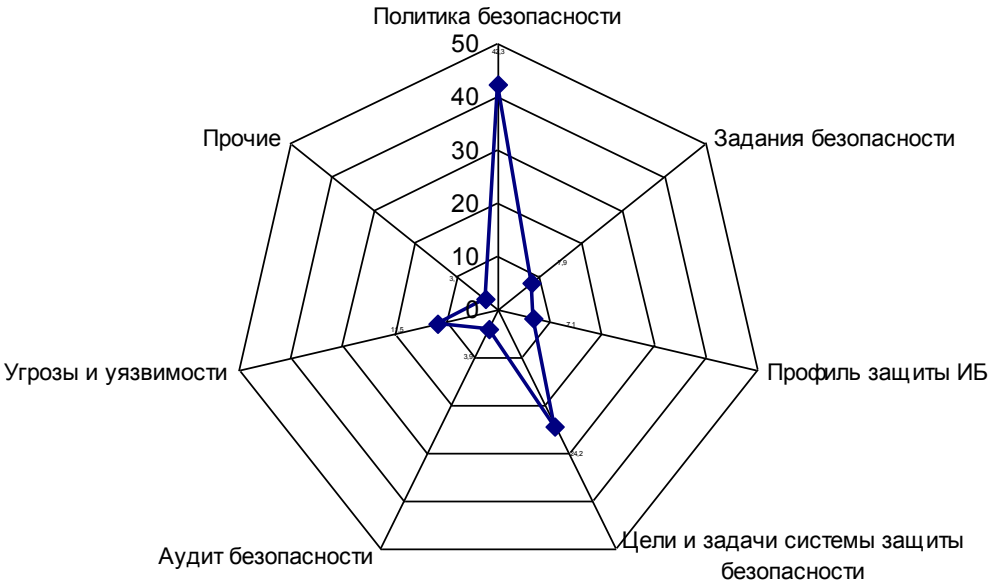


Рисунок 1 - Анализ результатов подготовки кадров к формированию профилей защиты информационной безопасности на рабочих местах

Общий анализ полученных результатов отражает тот факт, что в процессе обучения в высших учебных заведениях формируются базовые понятия назначения систем информационной безопасности, построение Политики безопасности, определение угроз и уязвимостей. В совокупности это определяет профиль знаний подготовки специалистов в области защиты информации от несанкционированного доступа и отражает низкий уровень сформированности таких понятий, как: "аудит безопасности", задания безопасности, профиль защиты информационной безопасности. Чтобы глубже понять суть этих вопросов и их прямое назначение, роль в обеспечении реализации Политики безопасности на предприятии, рекомендуем следующий алгоритм (рисунок 2 а, б).

На рисунке показан фрагмент поэтапного формирования навыков для построения Профилей защиты информационной безопасности. Это укрупненный поэтапный алгоритм. включающий подготовительный, основной и заключительный этапы. На заключительном этапе собственно и формируются навыки по созданию профилей защиты.

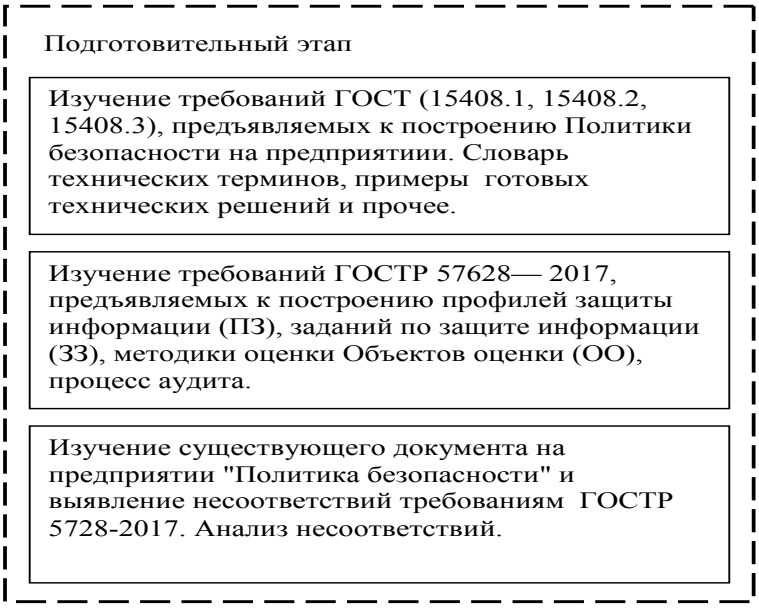


Рисунок 2(а) - Фрагмент подготовительного этапа формирования навыков подготовки к построению профилей безопасности

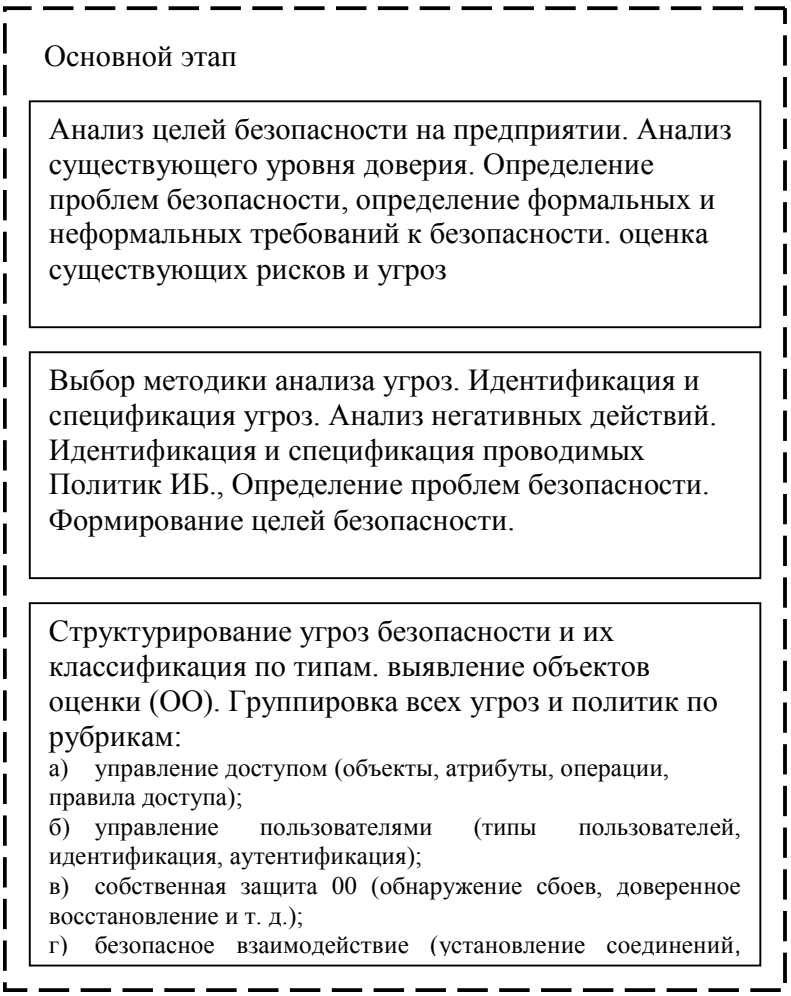


Рисунок 2(б) - Фрагмент алгоритма подготовки к построению Профилей защиты для предприятия на основном этапе

В соответствии с требованиями ГОСТ, предложенный алгоритм направлен на сбор требований, решение, по которым должны отражаться в Профилях защиты.

Таким образом, документ "Профиль защиты информационной безопасности", сформированный для деятельности производственных структур содержит следующие виды логически взаимосвязанной информации, созданной в результате поэтапного выполнения алгоритма:

1) формулировку потребности в безопасности, которая была сформулирована в результате выявленной проблеме безопасности;

2) описание проблемы безопасности, в которую включены перечень выявленных угроз со стороны внешней и внутренней среды;

3) "дерево целей" безопасности объектов оценки и "дерево возможных рисков" объектов оценки;

4) Логическая связка "Дерево требований" - "Дерево решений", в которой отражены функциональные требования доверия и безопасности, отражающие и уровень уверенности предприятия в принимаемых мерах по защите информации.

Приобретенные навыки построения профилей защиты позволят существенно снизить риски возникновения потерь информационных активов на предприятии.

Библиографический список

1. Методический документ ФСТЭК России «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» (ИТ.СКН.П4.ПЗ). 2014.

2. Методический документ ФСТЭК России «Профиль защиты средств контроля подключения съемных машинных носителей информации пятого класса защиты» (ИТ.СКН.П5.ПЗ). 2014.

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. Приказом ФСТЭК России 11.02.2013 № 17).

4. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Приказом ФСТЭК России 18.02.2013 N«21).

ОСОБЕННОСТИ ИДЕНТИФИКАЦИИ УГРОЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ДЛЯ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННЫХ СТРУКТУР

Глухова Л.В., д. э. н., профессор, Губанова С.Е., аспирант
Волжский университет имени В.Н. Татищева
г. Тольятти

Аннотация. *Развитие современных средств компьютерных коммуникаций привело к потребности более пристрастного изучения на рабочих местах конечных пользователей инструментария оценки угроз экономической безопасности. Одним из них является набор методик для оценки рисков информационной безопасности.*

В статье раскрыты некоторые подходы к идентификации угроз информационной безопасности в промышленных структурах.

Ключевые слова: *экономическая безопасность, угроза экономической безопасности, информационная безопасности, методика оценки рисков информационной безопасности.*

Экономическая безопасность – это возможность устойчивого функционирования и развития предприятия даже в условиях нестабильного и неблагоприятного внешнего окружения [1]. Она зависит от множества факторов и, по сути, представляет собой динамический процесс балансирования внешних и внутренних вызовов, рисков и угроз с помощью ответных (реактивных), а также упреждающих (проактивных) мер, реализуемых специалистами и менеджментом [2].

Понятно, что разные компании имеют разный набор и вес актуальных проблем, они находят отражение в их модели угроз и модели нарушителя, но вместе с тем есть типовые и долговременные угрозы и риски, свойственные большинству предприятий. Это стихийные и техногенные катастрофы, коррупция, некомпетентность, захват активов и т.д. Именно из-за их распространённости общество научилось как-то с ними управляться и противодействовать. Но есть угрозы новые, вызванные современными реалиями и оказывающие пагубное влияние на всех участников рынка. Стандарты взаимодействия с ними ещё не наработаны, и это сильно осложняет ситуацию [3].

Какие угрозы на сегодняшний день можно считать таковыми? Будем рассматривать этот вопрос в разрезе деятельности промышленных структур и идентификации угроз информационной безопасности как базовой компоненты экономической безопасности в условиях цифровизации и развитой информатизации в стране [4].

Выделим три группы факторов, по мнению авторов оказывающих наибольшее влияние на возникновение угроз экономической безопасности:

1) санкции, которым подверглась наша страна, и связанные с этим ограничения в плане финансирования, доступа к новым технологиям, взаимодействию с партнёрами; Отсюда – острая необходимость в импортозамещении;

2) кризис доверия, который сегодня очевиден во всех сегментах рынка – от государств до бизнеса и рядовых граждан, тормозящий и усложняющий коммуникации и развитие;

3) отсутствие упрощенных методик управления рисками информационной безопасно-

сти, что привело к актуализации проблем эффективного управления бизнес-процессами промышленных структур в условиях перехода страны к цифровизации. Это порождает множество локальных задач на рабочих местах, связанных с защищенностью информационных активов, которые сегодня выходят на передний план в вопросе ценности и условий конкурентоспособности.

То же самое можно переформулировать так: возросла необходимость формирования навыков применения инструментов менеджмента к снижению рисков и угроз информационной безопасности при переходе реального сектора экономики к цифровизации. Постоянное появление новых продуктов, информационных и коммуникационных сервисов с их возможностями и рисками. Где есть новая возможность – там есть и новый риск.

Все эти группы не изолированы, разумеется, и определённым образом стыкуются. Но всё-таки они сущностно разные. Назовем их условно: 1 группа - Экономика. 2 группа - Доверие. 3 группа - цифровые технологии как новый феномен, сопровождающий все современные бизнес-процессы (ЦТ).

И именно поэтому их интересно рассматривать и изучать, чтобы, в конечном итоге, найти пути и способы блокировки нежелательных ситуаций, ведущих к возможному возникновению экономических потерь.

Отметим, что постоянно возникающие риски сегодня неизбежны – они спутники неопределённости, а неопределённость в нашей жизни только растёт. Но в коммерческих, финансовых, сервисных и прочих постиндустриальных отраслях вероятность рисков обычно не так катастрофична, как для крупных промышленных структур, отягощённых, как правило, капитальными строениями, оборудованием, большим количеством сотрудников, и, соответственно, обязательств. Промышленные предприятия вынуждены быть более осторожны и консервативны относительно возможных рисков.

Рассмотрим две последние группы в классификационной структуре более подробно (это группы ЦТ и Доверие).

Группа ЦТ характеризуется следующими параметрами:

1. Быстро растёт сложность технологий, отсюда:

- пользователи не успевают их освоить до стадии "прочного владения навыками" и способностью "быстрого тиражирования" новых знаний;

- не хватает квалифицированных специалистов, что существенное "тормозит" процесс извлечения знаний и их обновления;

- сложности во взаимопонимании между специалистами и руководством, с одной стороны, и специалистами и рядовыми пользователями, с другой, что приводит к возникновению различных "рассогласованностей", "нестыковок", потребности "переделки и переработки" и прочих затрат на качество производственной деятельности.

- распространение мошеннических схем, которые в ввиду своей изощренности не сразу распознаются и происходит, в лучшем случае просто потеря времени, а в худшем - возникновение угрозы информационной безопасности.

2. Ряд технологий настолько удобны в использовании, что они распространяются, несмотря на изначальную их уязвимость в плане информационной безопасности (например, облачные технологии, облачный сервис, или использование мобильных устройств). Это приводит к потребности перестройки уже "налаженного" информационного и цифрового сервиса под новые реалии. Что влечет не только инициацию процессов мотивации в освоении перспективных ИТ-сервисов, но, и порождает потребность возникновении и развитии новых путей для совершенствования промышленной сферы.

3. Нарушители всегда идут на шаг впереди, находя и используя "дыры и слабые места" – например, «уязвимость нулевого дня». Здесь под этим термином понимается такая ситуация, при которой фиксируются неустраненные уязвимости, а также выявляются новые вредоносные программы, против которых еще не разработаны защитные механизмы

4. Отсутствие (или недостаток) признанных стандартов, когда менеджмент вынужден опираться строго на мнение экспертов, а каждый эксперт зачастую видит ситуацию по-

своему. Существующие стандарты в области менеджмента информационной безопасности, в частности менеджмента рисками в службах промышленных производственных структур зачастую не находят должного понимания и претворения в повседневные функции мониторинга.

Можно предложить к использованию также ИСО/МЭК ТО 13335-1:2004 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1 Концепция и модели управления безопасностью информационных и телекоммуникационных технологий (или Российский аналог ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Здесь даны основы, позволяющие выработать концепцию управления рисками, угрозами и уязвимостью [1-4, 7]

5. Видение специалистов промышленных структур при гармонизации торгово-промышленных отношений в условиях глобализации на возникновение дополнительных групп угроз. Их можно идентифицировать по следующим факторам:

- утечка информации, атаки на системы управления технологическими процессами и атаки на репутацию с помощью IT - фактора. В этом случае экономическую безопасность можно рассматривать в большей степени как информационную безопасность. Поскольку возникают угрозы целостности, конфиденциальности, доступности, фиксации авторства, атаки, вирусы, спам, и прочее;

- зависимость от ИТ-сервиса, передача контроля от человека к различным цифровым платформам, оптимизаторам и прочее (то есть уход от одних проблем – «человеческий фактор» - к другим – "роботизированный фактор": какие-то алгоритмы, в том числе самообучающиеся, будут определять результат).

- зависимость и неясные последствия от технологий «Интернет вещей», «Умный дом (город, производство и т.д.)", что требует новых, достаточно больших затрат на обучение и усвоение нового, которое, зачастую такими быстрыми темпами невозможно "уложить кирпичиками знаний" [5].

Группа "Доверие" характеризуется следующими особенностями:

- резкий рост сложности и порога освоения технологий мешает пониманию процессов со стороны рядовых пользователей, что способствует росту количества мошеннических схем от квалифицированных злоумышленников;

- асимметричность информации усложняет взаимодействие с партнёрами, клиентами и конкурентами;

- постоянные изменения нормативной базы;

- недостаточность доверия в оффлайне выталкивает транзакции в «цифру», то есть в онлайн (блокчейн, смарт-контракты, удалённое взаимодействие), порождая новые проблемы.

- использование самообучающихся алгоритмов в определённой степени выводит из-под контроля специалистов результаты их (алгоритмов) работы.

- сбор данных о пользователях и передача этих данных для разных целей.

- манипуляции на основе Больших данных.

Таким образом, можно сделать вывод, что для идентификации угроз экономической безопасности в производственных структурах должны находиться специалисты, имеющие навыки их обнаружения и локализации [6].

Для этого необходимо хорошо знать требования нормативных документов, например, требования недавно введенного стандарта ГОСТ Р 57628-2017. Специалисты кафедры "Менеджмент организации" готовы предложить для производственников и всех заинтересованных лиц курс обучения "Стандартизация требований к менеджменту рисков информационной безопасности". Его содержание направлено на формирование практических навыков по идентификации угроз информационной безопасности [8].

Библиографический список

1. Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 № Пр-1895) и Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

2. ГОСТ Р ИСО/МЭК 13335-1-2006 «Национальный стандарт Российской Федерации/ Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».

3. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

4. ГОСТ Р ИСО 31000-2010 «Менеджмент риска. Принципы и руководство».

5. Губанова, С.Е. Особенности работы корпоративного Удостоверяющего центра крупного промышленного предприятия // Информационные системы и технологии: управление и безопасность. Сборник статей II Международной заочной научно-практической конференции / Поволжский гос. ун-т сервиса – Тольятти - Русе: Изд-во ПВГУС. 2013 № 2, с. 185-191.

6. Глухова, Л.В. Губанова, С.Е. Некоторые аспекты менеджмента информационной безопасности промышленных комплексов. // Вестник Волжского университета имени В.Н. Татищева, 2015, № 3 (34), С. 135-144.

7. Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов. СТБ 34.101.67 [Электронный ресурс]. Источник: http://pki.gov.by/docs/Formats.pdf.

8. Глухова, Л.В. Информационно-аналитическая деятельность по обеспечению экономической безопасности // наука - промышленности и сервису. Тольятти: 2013, № 8-1. С. 154-157.

ПОДХОДЫ ТЕОРИИ КОММУНИКАЦИИ К АНАЛИЗУ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Благов Ю.В., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти
Арсентьева Е.Ф., д. ф. н., профессор
Волжский университет имени В.Н. Татищева
г. Тольятти
Казанский (Приволжский) федеральный университет
г. Казань

В современной теории коммуникации существует несколько научных подходов к изучению коммуникации. Во-первых, они разделяются на две группы: технократические и интеракционные. Такое разделение обусловлено существованием двух отличающихся парадигм самой коммуникации: механистической и деятельностной.

В механистической парадигме под коммуникацией понимается однонаправленный процесс кодирования и передачи информации от источника и приема ее (информации) получателем сообщения. В деятельностном подходе коммуникация понимается как совместная деятельность участников коммуникации (коммуникантов), в ходе которой вырабатывается общий (до определенного предела) взгляд на вещи и действия [2, с. 33].

Во-вторых, в рамках интеракционных теорий, которые развиваются в социологии, психологии, культурологи, ученые разделились в решении вопроса о том, как объяснить коммуникацию – ссылками на индивидуальную осознанную деятельность или в качестве производной от социальной структуры. Этот спор имеет давние корни и отражает проблему места и роли человека в обществе, соотношения объективного и субъективного в поведении людей.

К числу технократических теорий относят: теорию информационного общества (Д. Белл, Дж. Гэлбрейт), теорию коммуникационных технологий (Г.М. Маклюэн (1911-1980), математическая теорию коммуникации (К. Шеннон, У. Уивер), многочисленные теории коммуникации в организациях.

Отличительной особенностью интеракционного подхода является то, что он рассматривает коммуникацию как взаимодействие и является альтернативой не только технократизму, но и бихевиоризму. Бихевиоризма, сводившего ее к прямому воздействию сообщений коммуникатора на реципиента, где последний выступает лишь в качестве объекта реагирующего на воспринимаемую информацию.

При альтернативном понимании сущности коммуникации на первый план выдвигается активность реципиента как равноправного субъекта коммуникативной деятельности. В этом и состоит суть интеракционного подхода, который был сформулирован Т. Ньюкомбом в 1953 году [6, с. 87].

В целом суть интеракционного подхода состоит в следующем:

1) субъекты коммуникации равноправны и связаны взаимными ожиданиями и установками, а также общим интересом к предмету общения;

2) коммуникация рассматривается как реализация этого интереса с помощью передаваемых сообщений.

Первоначально исследования массовой коммуникации осуществляется в рамках социологии. Так, Р.Э. Парк, Ч.К. Кули, У. Липпман трактовали массовую коммуникацию как общение членов массы – “коллективной группировки” в условиях индустриального урбанизированного общества. Ими активно изучались и социальные функции массовой коммуникации.

Новым этапом в развитии теорий массовой коммуникации стало изучение воздействия

средств массовой коммуникации на аудиторию. Появились такие теории как теория селективной экспозиции, теория диффузии (распространения) инноваций, теория культивирования, теория информационных барьеров и др.

Изучение массовой коммуникации первоначально развивается как часть общесоциологической теории.

Массовые коммуникации рассматриваются как общение индивидов в пределах большого города, страны и даже мира в целом; когда они оказываются вырванными из привычных условий взаимодействия и действуют независимо от социальных ролей, определяемых их положением в обществе. Активно изучаются социальные функции массовой коммуникации [1, с. 131].

В анализе угроз информационной безопасности средствами массовой коммуникации особое место занимает телевидение, ставшее наиболее существенным культурным явлением XX века.

В анализе телевидения видное место занимает критика, обвиняющая его в формировании всевозможных видов нежелательного коммуникативного поведения. Так, нередко высказывается сожаление по поводу снижения культурного значения типографии и превращения телевидения в средство, вызывающее приятное состояние эйфории, но истощающее творческие способности.

Большой вклад в эти исследования внесла Анненбергская школа, созданная при Пенсильванском университете в 1959 году и возглавляемая профессором этого университета Джербнером. Школа ставила своей целью изучение СМИ, их роль в коммуникационном процессе, влияние на массовую аудиторию, на формирование культурных стереотипов общества. Анализируя деятельность средств массовой коммуникации, в первую очередь телевидения, специалисты Анненбергской школы выделили две их ключевые и связанные друг с другом функции — социальной интеграции и социализации. Выполняя эти функции массмедиа выступают в качестве средства сохранения целостности сложившихся общественных отношений и структур. Внедряя в массовое сознание определенные культурные стереотипы и целенаправленно формируя определенный тип личности, они тем самым способствуют закреплению и сохранению сложившейся системы общественных связей [7, с. 105]. Раньше эти функции выполняли мифология, фольклор и религия, в настоящее время они главным образом возложены на телевидение, вводящее массового зрителя в мир особой условной культуры с ее представлениями о жизненных ценностях и порядках.

Массированное и всеохватное воздействие медийных средств создает массовую аудиторию со стандартным потребительским видением мира и образом жизни, какой не могло быть в доэлектронную эпоху. При этом они ориентируют аудиторию не столько на творческую развивающую деятельность, сколько на потребительско-развлекательные стандарты, нивелирующие личность, делающие ее маловосприимчивой ко всему оригинальному, неординарному, требующему интеллектуальных усилий. Более того, мотивы насилия, ставшие неотъемлемой частью современной телекультуры, по мнению специалистов, с одной стороны, разлагают общественные нравы, порождают агрессивность, а с другой — вызывают чувство страха, которое, по мнению специалистов, может оказаться даже более опасным, чем агрессия [1, с. 52].

Теории волшебной пули и подкожных инъекций, или «лекарственного средства для подкожных инъекций», согласно этим теориям, те, кто управляет средствами информации, управляет обществом, поскольку средства информации имеют прямое, непосредственное и мощное воздействие на тех, кто обращают внимание на их содержание.

В соответствии с *теорией аккумуляции* сила и эффективность воздействия средств информации на людей прямо пропорциональны частоте информационных «инъекций».

С 1920-х гг. теории массовой коммуникации начинают испытывать все большее влияние эмпирических исследований. В этих исследованиях эффективность коммуникации рассматривалась как прямое следствие единичного или повторяющегося пропагандистского воздействия, и выяснились факторы, усиливающие или ослабляющие его.

Теория селективной экспозиции, которая утверждала, что аудиторию нельзя представлять как послушную массу, некритически воспринимающую любую информацию. Каждый человек (как личность, как индивидуальность) имеет собственные вкусы, предпочтения и интересы, в соответствии с которыми осуществляет выборочное потребление информации, предлагаемой СМИ.

Во-вторых, в 1940 году П. Лазарсфельдом и Б. Берельсоном было установлено наличие *двухступенчатого потока информации (двухступенчатая модель коммуникации)* была выдвинута нашедшая эмпирическое подтверждение гипотеза о том, что сообщение, посланное аудитории, достигает сначала «лидера мнения» (наиболее авторитетного члена группы) внутри группы, а затем уже через него других членов данной группы [4, с. 102].

«Лидеры мнения» в социологии стали рассматриваться как связующее звено между средствами массовой коммуникации и массой, нуждающейся в ориентации. Последующие исследования привели к модификации данной теории и созданию концепции многоступенчатого потока информации, так как выяснилось, что «лидеры мнений» имеют в свою очередь собственных «лидеров мнений» и обращаются к ним за информацией [2, с. 47].

Теория, получившая название *«спираль тишины / молчания»,* развитая Э. Ноэлль-Нойманн, напоминает о «парадоксе голосования», согласно которому многие не участвуют в выборах, поскольку полагают, что их «голос» не является решающим.

Теория диффузии (распространения) инноваций разрабатывалась Э. Роджерс в 1960-е гг. Диффузия понимается как процесс, при котором новшество распространяется в обществе через коммуникационные каналы в течение определенного времени.

Теория культивирования возникла на основе научно-исследовательской работы Дж. Гербнера и его коллег из Анненбергской школы в области «культурных индикаторов» (середина 1960-х гг.), среди которых центральное место занимали средства массовой информации и в первую очередь телевидение. Массмедиа в целом рассматривались как средства, культивирующие (укрепляющие) установки и ценности, которые уже существуют в культуре. Согласно выдвинутой гипотезе, телевидение рассматривалось как средство, нацеленное на долгосрочный эффект, составленный из небольших, постепенных, косвенных эффектов, накапливающихся и приводящих к существенному изменению своего значения.

Теория информационных барьеров разрабатывалась социологом и социальным психологом К. Левином, предложившим новый термин — «контролер», «привратник». Теория носит преимущественно прикладной характер и может быть отнесена к процессам выбора новостей. В ее основе лежит предположение, что прохождение информации по некоторым каналам коммуникации зависит от наличия в них «ворот» (аналог Цензуры), которые в свою очередь управляются некими «контролерами».

Это предположение также нашло отражение в *теории искажения новостей* (первоначально сформулированной У. Липпманом, согласно которой общественность откликается не на фактические события в окружающем мире, а на события в псевдомире, так как изображения внешнего мира в человеческом сознании, ошибки и ограниченность журналистов создают ложный образ мира.

Теория обретения пользы и удовлетворения, представленная в конце 1950-х гг. Дж. Бламлером и Э. Кацем и близкая теории селективной экспозиции, утверждала, напротив, что зрители отнюдь не пассивно воспринимают сообщения средств массовой информации. Члены аудитории, согласно данной теории являются активными отборщиками сообщений, ориентируемыми своими целями, потребностями, интересами, ценностными ориентациями [5, с. 29]. Активность потребителя информации обусловлена также внешними обстоятельствами, к которым в первую очередь относится конкуренция средств массовой коммуникации.

Теория зависимости, показывает наличие сложной системы взаимодействий между средствами информации, их аудиторией и обществом в целом, а также устанавливает существование сильной зависимости потребностей и целей людей от деятельности средств массовой информации [3, с. 95].

Таким образом, подходы теории коммуникации к анализу угроз информационной безопасности средства массовой коммуникации не столько заставляют людей думать, сколько формируют их отношение к событиям. Повестка дня носит запрограммировано-выборочный характер, поскольку и темы, и проблемы, прежде чем они станут достоянием массовой аудитории, подвергаются тщательному отсеву и распределяются в соответствии с той степенью значимости в информационном пространстве, которая им предназначается самими СМИ.

Библиографический список

1. Березин, В.М. Массовая коммуникация: сущность, каналы, действия / В.М. Березин. – М.: РИП - холдинг, 2003. – 174с.
2. Василик, М.А. Основы теории коммуникации / М.А. Василик. – М.: Гардарики, 2003. – 615 с.
3. Ганатюк, О.Л. Основы теории коммуникации / О.Л. Ганатюк. – М.: Кнорус, 2012. – 256 с.
4. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. – М.: Энергоатомиздат, 2004. – 400с.
5. Почепцов, Г.Г. Теория коммуникации / Г.Г. Почепцов. – М.: Ваклер, 2006. – 656 с.
6. Современные бизнес-коммуникации / В.А. Спивак. – СПб: Питер, 2001. – 448 с.
7. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. / А.Ю. Щербаков − М.: Книжный мир, 2009. – 352 с.

РОЛЬ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ ВОЙНАХ

Витковская Н.Г., к. п. н., доцент
Волжский университет имени В.Н. Татищева
г. Тольятти

С развитием информационного общества появилось и новое оружие с аналогичным названием, которое вылилось в уже привычное нам словосочетание «информационная война». Информационные войны велись задолго до XX века. В далеком прошлом люди умели влиять друг на друга только в процессе непосредственного общения, оказывая воздействие на своих собеседников посредством слов, интонации, жестов, мимики. Сегодня способы воздействия на человеческое сознание стали намного более разнообразными, действенными и изощренными благодаря накопленному за тысячелетия практическому опыту, а также за счет создания специальных технологий общения, взаимодействия и управления людьми. Поэтому информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере. Применение информационного оружия означает прежде всего работу с общественным мнением, с идеологией противника.

Настоящая тема исследования является актуальной, поскольку необходимо осознать природу и технологии информационной власти над людьми, бесконтрольность которых может привести не только к массовому истреблению отдельных народов, но и к гибели современной цивилизации в целом. Для отпора информационной агрессии необходимо прежде всего понимание сути происходящих событий. В настоящее время осуществляется глобальная информационно-культурная и информационно-идеологическая экспансия Запада, осуществляемая по мировым телекоммуникационным сетям и через средства массовой информации. Многие страны вынуждены принимать специальные меры для защиты своих сограждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния. Возникает необходимость защиты национальных информационных ресурсов и сохранения конфиденциальности информационного обмена по мировым открытым сетям, так как на этой почве могут возникать политическая и экономическая конфронтация государств, новые кризисы в международных отношениях. Поэтому информационная безопасность, информа-

ционная война и информационное оружие в настоящее время оказались в центре всеобщего внимания.

Реалии сегодняшнего дня таковы, что мы всё больше говорим об «информационной войне», о её связи с психологическим давлением и манипуляцией гражданским обществом. Известно, что противоборство идеологий и психологические конфликты имели место всегда, ещё во времена античности. Война идей сопровождала каждый вооружённый конфликт, примеры которых в истории можно найти в огромном количестве. Под информационной войной теоретик С. Падовер понимает несколько иной тип воздействия, чем тот, который многие десятилетия именовался психологической войной, определяемой как «использование всех возможных видов коммуникации с целью уничтожения желания врага сражаться» [4, с. 23].

В связи с появлением новых задач после окончания «холодной войны» термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года [6, с. 276].

Таким образом, в число сфер ведения боевых действий помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «human network») [1, с. 47].

Наиболее полное определение информационной войны даёт, на наш взгляд, исследователь И.Н. Панарин. «Информационная война - комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника» [5, с. 39].

Информационная война состоит из действий, предпринимаемых с целью достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

«Система рассуждений противника, отталкиваясь от новых элементов, должна прийти к новым решениям. Всякое сопротивление партнера говорит о том, что полученная им информация оказалась недостаточно эффективна. Тогда, чтобы продолжать борьбу нужно опять выдавать информацию – более значительную, чем выданная ранее, чтобы добыть в обмен информацию о том, что выданная достигла цели. Это выражается в приведении новой, более веской аргументации. Наступающий выдает все новую и новую информацию» [6, с.9]. Реально по этой модели развивается любая информационная кампания. При этом интересно, что основные факты особо не меняются, наращивание новой информации идет на периферии основного обвинения, включая новые дополнительные подтверждения при сохранении старой линии.

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном фронте, либо в экономической, политической или социальной сферах [3, с. 27].

У современного человека есть возможность оперативно получать огромный объем информации со всего света. Но, как правило, это та информация, которая поступает через средства массовой информации. Человек видит мир глазами СМИ, в его голове формируется такая картина действительности, которую предлагают ему СМИ. В таких условиях появляются

огромные возможности по манипулированию массовым сознанием, созданию мифов. Находясь часто в мире оторванных от реальности символов, люди могут идти даже против своих собственных интересов.

В связи с этим можно выделить следующие методы информационной войны:

- скрытие существенной информации;
- информационный мусор;
- смещение понятий;
- отвлечение внимания;
- применение ничего не значащих понятий;
- негативная информация сама себя продает, а за позитивную кто-то должен платить;
- ссылка на несуществующие основания;
- информационные табу;
- прямая ложь.

Средства массовой коммуникации формируют «массового» человека нашего времени. В то же время они разобщают людей, вытесняют традиционные непосредственные контакты, заменяя их телевидением и компьютерами. В работе С. Кара-Мурзы «Манипуляция сознанием» приведены характерные черты такого «массового» человека. Там же отмечается, что одновременное распространение противоречивых взаимоисключающих суждений затрудняет адекватную ориентацию, порождает безразличие и апатию, провоцирует некритичность, возникает социальная дезориентация: большее впечатление производит не аргументированный анализ, а энергичное, уверенное, пусть и бездоказательное, утверждение. На этом фоне отмечается снижение способности к концентрации. «Массовый» человек импульсивен, переменчив, способен лишь к относительно краткосрочным программам действия. Он часто предпочитает иллюзии действительности [2, с. 129–212].

Информационное оружие – наиболее эффективное оружие современности. Между тем, его применение не регламентируется международным правом. Информационная война характеризуется отсутствием линии фронта, стиранием четких границ между государствами, между войной и миром, между участниками и неучастниками боевых действий.

Таким образом, принципиальное отличие информационного оружия от обычного в том, что воздействует оно на разум, дух, а не на тело человека.

У современного человека есть возможность оперативно получать огромный объем информации со всего света. Но, как правило, это та информация, которая поступает через средства массовой информации. Человек видит мир глазами СМИ, в его голове формируется такая картина действительности, которую предлагают ему СМИ. В таких условиях появляются огромные возможности по манипулированию массовым сознанием, созданию мифов. Находясь часто в мире оторванных от реальности символов, люди могут идти даже против своих собственных интересов.

Библиографический список

1. Гриняев, С.Н. Информационная война: история, день сегодняшний и перспектива / С.Н. Гриняев. – М.: Аспект Пресс, 2001. – 97 с.

2. Кара-Мурза, С.Г. Манипуляция сознанием / С.Г. Кара-Мурза. – М.: Алгоритм, 2000. – 204 с.

3. Манойло, А.В., Петренко А.И. Информационно-психологическая безопасность современного информационного общества / А.В. Манойло, А.И. Петренко. – М.: Институт психологии РАН, 2003. – 42 с.

4. Падовер, С.К. Психология войны / С.К. Падовер. – М.: Луч, 1960. – 238 с.

5. Панарин, И.Н. Технология информационной войны / И.Н. Панарин. – М.: КСП+, 2003. – 320 с.

6. Черешкин, Д.С. Проблемы управления информационной безопасностью / Д.С. Черешкин. – М.: Топа, 2002. – 192 с.

7. Энгдаль, У.Ф. Столетие войны / У.Ф. Эндгаль. – М.: Нико-пресс, 2008. – 406 с.

СОДЕРЖАНИЕ

ПРАВОВАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В СМИ

ВЕСТНИК
ПО БЕЗОПАСНОСТИ

Выпуск одиннадцатый

Компьютерная верстка и дизайн О.Ю. Федосеева, И.А. Чиргадзе

Сдано в набор 14.12.2018.
Подписано к печати 16.12.2018.
Формат 60x84/16. Бумага офсетная.
Гарнитура Times ET.
Печать офсетная. Усл. п.л. 13,3.
Тираж 500 экз. Заказ № 2.