

Сури́н Влади́мир Влади́мирович, к.ю.н., доцент,
декан факультета внебюджетного образования,
ФКОУ ВО Пермский институт ФСИН России,
г. Пермь

**АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ
В ПЕНИТЕНЦИАРНЫХ УЧРЕЖДЕНИЯХ
ASPECTS OF INFORMATION PROTECTION
IN PENITENTIARY INSTITUTIONS**

Аннотация: в статье исследуется содержание термина «защита информации в пенитенциарных учреждениях». Рассматриваются различные теоретические подходы, существующие по данному вопросу, а так же практика его использования.

Abstract: the article examines the content of the term "information protection in penitentiary institutions". The various theoretical approaches that exist on this issue, as well as the practice of its use, are considered.

Ключевые слова: защита информации, информационная безопасность, исполнение наказаний.

Keywords: information protection, information security, execution of punishments.

Уголовно-исполнительная система (УИС) является органом исполнительной власти, осуществляющим правоприменительные функции, функции по контролю и надзору в сфере исполнения уголовных наказаний в отношении осужденных, функции по содержанию лиц, подозреваемых либо обвиняемых в совершении преступлений, и подсудимых, находящихся под стражей, их охране и конвоированию. В любом государстве УИС в своей деятельности руководствуется соответствующими законами, актами органов исполнительной власти, международными договорами и т. д.

В упомянутых документах, в частности, ставится задачи по обеспечению защиты сведений, составляющих государственную, служебную и иную охраняемую законом тайну, в уголовно-исполнительной системе. Это объясняется наличием ряда противоречий между интересами сотрудников УИС и осуждённых, что порождает необходимость ограничения доступа к определённой информации, возникающей в деятельности пенитенциарных органов.

В месте с этим, как показывает статистика последних лет, с одной стороны, остаётся непростой криминогенная обстановка внутри исправительных учреждений, в том числе, фиксируются попытки незаконного доступа к служебным сведениям. С другой стороны, широкое распространение современных информационных технологий создаёт благоприятную обстановку для попыток незаконного ознакомления со сведениями конфиденциального характера, отражающих работу учреждений уголовно-исполнительной системы.

В сложившихся условиях особую актуальность имеет деятельность, направленная на защиту конфиденциальных сведений, используемых сотрудниками УИС. Решение этой проблемы предусматривает много аспектов, один из них это определение самого понятия и его особенности в условиях деятельности УИС.

«Защита информации» может быть определена разными способами, за основу возьмём законодательное определение, согласно ему: «Защита информации представляет собой принятие правовых, организационных и технических мер» [1]. Таким образом, в данном понятии выделяется три составные части: правовой, организационный и технический аспекты. Рассмотрим, кратко, каждый из них.



Правовой аспект или «правовое обеспечение». В юридической литературе содержание данного понятия понимается неоднозначно [2, с. 6]. Одними из значимых трудов, посвященных постановке и рассмотрению данной проблемы, являются работы В.А. Козбаненко [3, с. 20]. Автор теоретически обосновал разграничение базовых юридических категорий «правовые основы», «правовое регулирование», «правовое обеспечение», выявил сущность и содержание этих терминов. При этом под правовым обеспечением В.А. Козбаненко предлагает понимать систему социально-правовых элементов и юридически значимых мер (средств, приемов и способов), влияющих на формирование и реализацию права.

Понятие «правовое обеспечение» можно рассматривать в широком и узком смысле слова. В широком смысле этим термином охватывается весь процесс выработки средств юридической регуляции и использования их в практической деятельности субъектов права для достижения фактических результатов в конкретной сфере общественных отношений. Важнейшими элементами здесь выступают, во-первых, правотворчество, во-вторых, правоприменение как комплексная властная деятельность по реализации правовых норм, в-третьих, правовая культура субъектов права, применительно к личности каждого гражданина, означает сочетание знания и понимания права с осознанным исполнением его предписаний.

В узком смысле слова правовое обеспечение защиты информации представляет собой совокупность нормативных правовых актов, регулирующих организацию и деятельность подразделений уголовно-исполнительной системы по использованию ими служебных сведений. Источниками нормативной правовой информации традиционно являются: международно-правовые акты; правовые акты общегосударственного уровня, которые в свою очередь могут делиться на законодательные и подзаконные; документы, принимаемые на уровне региональных органов власти; акты местного самоуправления.

Организационный аспект определяет правила сбора, поиска, документирования, передачи, хранения, тиражирования информации и многие другие вопросы, связанные с циркулированием сведений различного характера, имеющих отношение к процессам исполнения и отбывания наказаний.

Данный круг вопросов представляется чрезвычайно широким. Одной его особенностью является тот факт, что реализация данных мероприятий, направленных на защиту информации в УИС во многом зависит от внешних условий, одним из которых является наличие осужденных и их определённый интерес к рассматриваемой проблеме. По своему характеру поведение осужденных может быть социально полезным, нейтральным с социальной точки зрения и общественно опасным [4, с. 132]. В зависимости от этого органам уголовно-исполнительной системы придётся реализовывать разный по объёму и характеру круг организационных мероприятий, направленных на защиту информации.

Обратим теперь своё внимание на технический аспект процесса защиты информации. Эта сфера тесным образом переплетается с только что рассмотренными вопросами. Вместе с тем, технический аспект требует несколько изменить акцент исследования. С нашей точки зрения основными элементами здесь являются: комплексное информационное, программное, аналитическое, научно-техническое и нормативно-методическое обеспечение стабильного функционирования, развития и совершенствования УИС; осуществление прикладных научных исследований и разработок в сфере информационных, социальных, экономических, инженерно-технических, технологических и иных проблем деятельности подразделений УИС; проведение работ по созданию и поддержанию в актуальном состоянии информационного ресурса УИС на основе внедрения современных информационных технологий; осуществление экспериментальных разработок на основе результатов научных исследований и опытно-



конструкторских работ, направленных на создание новой продукции, процессов, программных средств, в интересах совершенствования и повышения эффективности деятельности подразделений УИС и др.

С нашей точки зрения, весьма важно, обратить внимание ещё на одну составляющую исследуемого понятия – сам термин «информация». Анализ содержания данного понятия показывает, что сложно сформулировать универсальные правила, применимые ко всем видам информации. Весьма целесообразным представляется использование другого термина – «информационный объект» который можно определить как единство (массив) информации, являющийся объектом конкретных правоотношений.

Если посмотреть на специфику реализации вышеперечисленных элементов в условиях деятельности УИС, не трудно заметить, что правовой аспект, в большем объёме реализуется не самими пенитенциарными органами, а иными субъектами права, прежде всего, органами власти, имеющими законотворческие функции. В отличие от данного аспекта, следующие два, а именно организационный и технический, в большей степени реализуются в своей деятельности самими сотрудниками УИС.

В большинстве стран процесс исполнения наказаний имеет своей целью восстановление социальной справедливости, а также исправление осужденных и предупреждение совершения новых преступлений [5].

Это обстоятельство обуславливает направленность процесса «защиты информации» в деятельности УИС. Как следует из вышесказанного данная деятельность должна служить частной и общей профилактике преступлений и правонарушений как среди осуждённых, так и среди лиц, освобождающихся от отбывания наказания. С одной стороны, осуждённые не должны быть осведомлены о тех сведениях, которые являются основой организации режима исполнения наказаний, с другой стороны, осуждённым не должны быть доступны сведения, используя которые они могли бы совершить преступления. Вместе с тем, работа по защите информации должна способствовать исправлению осуждённых, в частности, ограждать его от стрессовых сведений, способных подтолкнуть к совершению необдуманных поступков [6, с. 82].

Таким образом, защита информации в деятельности УИС представляет собой комплекс правовых, организационных и технических мер, направленных на определение правового режима информационных объектов, использующихся в пенитенциарной сфере, с целью восстановления социальной справедливости, а также исправления осужденных и предупреждения совершения новых преступлений.

Список литературы:

1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// "Российская газета", N 165, 29.07.2006
2. Правовое обеспечение предпринимательства. Учебное пособие. Под ред. М.П.Ринга. – М., МИЭП. 1996. – С. 6.
3. Козбаненко В.А. Правовое регулирование и правовое обеспечение государственного управления: сущность и содержание. Учебно–метод. Пособие. – М.: ИПКГосслужбы, 2002. – С.20.
4. Филимонов В. Д., Филимонов О. В. Правоотношения. Уголовные правоотношения. Уголовно-исполнительные правоотношения. – М.: «ЮрИнфоР-Пресс», 2007. – С.20.
5. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ // "Собрание законодательства РФ", 17.06.1996, N 25, ст. 2954; "Уголовно-исполнительный кодекс Российской Федерации" от 08.01.1997 N 1-ФЗ // "Российская газета", N 9, 16.01.1997.
6. Wortley, R. Situational prison control / Richard Wortley. – Cambridge university press, 2002. – С.82

