УДК 332.02

Сосипатров Р.А.,
магистрант,
ИФ РАНХиГС,
Российская Федерация, Иваново
Бабаев Д.Б., к.э.н., доц.
научный сотрудник,
ИФ РАНХиГС
Российская Федерация, Иваново

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОМ И МУНИЦИПАЛЬНОМ УПРАВЛЕНИИ: ОБЩАЯ ОЦЕНКА ЗАКОНОДАТЕЛЬСТВА

Аннотация. *В современном мире информация является одним из важнейших ресурсов. Оперативная обработка больших массивов данных в органах государственной власти является гарантией принятия эффективных управленческих решений, поэтому защита информации от несанкционированного доступ, искажения и компрометации является одной из приоритетных задач в области государственного и муниципального управления (ГИМУ). Статья посвящена общей оценке законодательства в области обеспечения информационной безопасности в ГИМУ.*

Ключевые слова*: защита информации, информационная безопасность, информационные технологии, информация, государственное и муниципальное управление.*

Sosipatrov R.A.,
master's student,
IB of RANEPA,
Russian Federation, Ivanovo
Babaev D.B., Ph.D., Assoc. Prof.,

Researcher,

IB of RANEPA

Russian Federation, Ivanovo

Ensuring information security in state and municipal administration: general assessment of legislation

Annotation. In the modern world, information is one of the most important resources. Prompt processing of large amounts of data in public authorities is a guarantee of effective management decisions, therefore, protecting information from unauthorized access, distortion and compromise is one of the priority tasks in the field of state and municipal administration (SMMU). The article is devoted to the general assessment of the legislation in the field of information security in the State Institute of Medical Management.

Key words: information protection, information security, information technology, information, state and municipal management.

Как известно, информационная безопасность представляет собой «практику» по предотвращению несанкционированного доступа к информации, несанкционированного ее модифицирования или уничтожения, записи (клонирования), использования и т.п. Поддержание информационной безопасности важно как для отдельных граждан, которые могут столкнуться с кражей своих личных данных, денег, или всей «цифровой личности» на одном или нескольких ресурсах, так и для организаций. Коммерческие организации и организации государственного и муниципального управления (ГИМУ) могут неожиданно получить существенные потери в том случае, если будут пренебрегать требованиями информационной безопасности. Отметим, что для организаций, в частности, организаций ГИМУ, требования информационной безопасности несколько модифицируются по сравнению с требованиями граждан – информационная безопасность должна обеспечивать доступность данных для работы с ними при одновременном соблюдении целостности данных и

обеспечении их конфиденциальности. Фактически в рамках информационной безопасности необходимо оценить риски, связанные с информацией и возможным к ней доступом, риски, связанные уничтожением информации и модификацией информации и т.п., а затем на практике организовать управление этими рисками, включая превентивное управление.

Поскольку сама по себе информационная безопасность является исключительно важным моментом, для ее организации в масштабах государства необходимы иерархически выдержанная система законодательных актов и механизмы, обеспечивающие функционирование информационной безопаности. В данной статье мы попытаемся оценить совокупность нормативных актов Российской Федерации по информационной безопасности и указать на ряд механизмов по ее реализации.

Говоря об информационной безопасности, в первую очередь, необходимо отметить, что в Российской Федерации существует целостная система нормативных документов, посвященная информационной безопасности, со своей иерархией. На «вершине» находится Доктрина информационной безопасности Российской Федерации»,[1] в которой определены основные цели, которые необходимо достигнуть для обеспечения национальной безопасности в информационной сфере, причем представлена совокупность иерархически зависимых друг от друга целей. Одними из ключевых целей являются разработка и использование отечественного программного обеспечения (ПО)[2] и подготовка

[1] Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (режим доступа 1.02.2021).

[2] Приоритетные направления поддержки проектов по разработке и внедрению отечественного программного обеспечения в рамках сквозных цифровых технологий (высокотехнологичных направлений) в 2020 году (утверждены протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27 августа 2020 г. No 17). URL: https://digital.gov.ru/uploaded/files/prioritetnyie-napravleniya-podderzhki-proektov-po-razrabotke-i-vnedreniyu-

квалифицированных специалистов в области IT-сферы[3]. Так, Н. Никифоров, министр цифрового развития, связи и массовых коммуникаций в период 2012-2018 гг. в рамках доклада на Гайдаровском форуме еще в 2016 году отмечал, что государство является важным инфраструктурным инвестором современной экономики.[4] Это, в принципе, соответствует основным положениям Доктрины, «под которую», если так можно выразиться, разработана совокупность нормативных документов.

Как и любая другая сфера деятельности, обеспечение информационной безопасности должно быть четко регламентировано нормативно-правовыми актами – и в этом ракурсе Российская Федерация следует общемировым тенденциям – определены среди приоритетных направлений в принимаемых на национальном уровне концептуальных документах развитие российских информационных и коммуникационных технологий, в том числе искусственного интеллекта, робототехники, биотехнологий, сетей связи нового поколения, обработки больших данных, Интернета вещей, индустриального Интернета и иные важные направления.

Можно говорить также о существовании ряда видов обеспечения информационной безопасности. Весьма важным является организационно-правовое обеспечение информационной безопасности, которое представляет собой совокупность управленческих решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и

otechestvennogo-programmnogo-obespecheniya-v-ramkah-skvoznyih-tsifrovyih-tehnologij-vyisokotehnologichnyih-napravlenij-v-2020-godu.pdf (режим доступа 1.02.2021).

[3] Ученые достаточно давно озабочены данной проблемой. По данному вопросу см., напр.: Васильев В.Н., Парфенов В.Г. Подготовка высококвалифицированных специалистов в области разработки программного обеспечения // Компьютерные инструменты в образовании. №1. 2012. С.48-56.

[4] Николай Никифоров выступил на Гайдаровском форуме // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Официальный сайт. URL: https://digital.gov.ru/ru/events/34523/ (режим доступа 1.02.2021).

функционирование систем защиты информации на конкретных объектах[5].

В процессе анализа можно прийти к выводу, что нормативно-правовое регулирование информационной безопасности в Российской Федерации в целом в настоящее время находится на достаточно высоком уровне. Основными, если так можно выразиться, «регуляторами» в сфере информационной безопасности в настоящее время являются следующие структуры высшего уровня управления: Федеральная служба безопасности Российской Федерации (ФСБ России), Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифра), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Федеральная служба по техническому и экспортному контролю (ФСТЭК России)[6] и др. Можно подтвердить, что они поддерживают издаваемые ими нормативно-правовые акты в актуальном состоянии, откликаясь на изменения, производимые в федеральном законодательстве.

Отметим ряд важнейших в плане нормативно-правого регулирования информационной безопасности нормативных документов: Указ Президента РФ от 16.08.2004 N 1085 (ред. от 31.08.2020) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка)[7]; Приказ ФСТЭК России от 12.05.2005 N 167 (ред. от 26.04.2018) "Об утверждении Регламента Федеральной службы по техническому и экспортному контролю" (Зарегистрировано в Минюсте

[5] По теории данного вопроса см., напр.: Аксенов С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Безопасность бизнеса. - М.: Юрист, 2008, № 3. - С. 5-10

[6] См., напр. по данному вопросу: Справочная информация: "Структура и функции федеральных органов исполнительной власти и управления" (Материал подготовлен специалистами КонсультантПлюс). URL: http://www.consultant.ru/document/cons_doc_LAW_120971/ (режим доступа 1.02.2021).

[7] Указ Президента РФ от 16.08.2004 N 1085 (ред. от 31.08.2020) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_14031/ (режим доступа 1.02.2021).

России 06.06.2005 N 6682)[8]; Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ[9]; Указ Президента РФ от 11.08.2003 N 960 (ред. от 03.07.2018) "Вопросы Федеральной службы безопасности Российской Федерации"[10]; Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 30.01.2021) "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации"[11]; Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.12.2020) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"[12]; есть и ряд других важных нормативных документов. Предполагается, что издаваемые в настоящее время нормативные акты должны находиться в русле реализации Государственной программы Российской Федерации «Информационное общество»[13].

Однако, отдельные важные аспекты защиты информации, обозначенные в нормативно-правовых документах федерального уровня, не всегда находят свое отражение в документах на уровне федеральных организаций и субъектов РФ, что, безусловно, ведет к некоторой

[8] Приказ ФСТЭК России от 12.05.2005 N 167 (ред. от 26.04.2018) "Об утверждении Регламента Федеральной службы по техническому и экспортному контролю" (Зарегистрировано в Минюсте России 06.06.2005 N 6682) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_53859/ (режим доступа 1.02.2021).

[9] Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_6300/ (режим доступа 1.02.2021).

[10] Указ Президента РФ от 11.08.2003 N 960 (ред. от 03.07.2018) "Вопросы Федеральной службы безопасности Российской Федерации" // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_43763/ (режим доступа 1.02.2021).

[11] Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 30.01.2021) "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации"// Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_77387/ (режим доступа 1.02.2021).

[12] Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.12.2020) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_85889/ (режим доступа 1.02.2021).

[13] Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 16.12.2020) "Об утверждении государственной программы Российской Федерации "Информационное общество" (с изм. и доп., вступ. в силу с 26.12.2020) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_162184/42f381c81a151303511bc36ecea815d2fb3050fe/ (режим доступа 1.02.2021).

противоречивости в решении вопросов защиты информации. Эти вопросы достаточно длительное время беспокоят как теоретиков, так и практиков[14].

Кроме вышеописанного организационно-правового обеспечения информационной безопасности можно также выделять программно-техническое обеспечение информационной безопасности (иногда принято выделять здесь два разных самостоятельных аспекта – программное и техническое обеспечение). В последнее время основные регуляторы в сфере информационной безопасности все чаще обращают внимание на, если можно так выразиться, «практическую защищенность» информационных систем государственных и муниципальных органов власти от потенциальных угроз и вредоносных воздействий. Информация, содержащаяся в информационных системах, защищается в соответствии с действующим законодательством Российской Федерации об информации и информационных технологиях. Программно-технические средства информационной системы должны иметь действующие сертификаты, выданные ФСБ и (или) ФСТЭК в отношении входящих в их состав средств защиты информации, включающих программно-аппаратные средства, средства антивирусной и криптографической защиты информации и средства защиты информации от несанкционированного доступа, уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий в отношении такой информации.

В том случае, если в рамках информационных систем не содержатся сведения, составляющие государственную тайну, внедрение, эксплуатация и развитие системы защиты информации производится в соответствии с Приказом ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных

[14] По данному вопросу см., напр.: Остапенко В.С. Информационная безопасность региональных органов исполнительной власти // Государственное и муниципальное управление. Ученые записки СКАГС. Р-н/Д: СКАГС, 2009. С.160-169.

информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (с изм. и доп., вступ. в силу с 01.01.2021)[15].

Предполагается, что для обеспечения защиты информации необходимо сформировать требования к защите информации, содержащейся в государственных информационных системах, применять сертифицированные средства защиты информации при ее передаче по информационно-телекоммуникационным сетям. Орган исполнительной власти, являющийся оператором информационной системы, должен обеспечить предотвращение несанкционированного доступа к информации, проводить мониторинг на предмет обнаружения фактов несанкционированного доступа к информации, предотвращать несанкционированное воздействие на входящие в состав информационных систем технические средства обработки информации, в результате которого нарушается их функционирование, осуществлять непрерывный контроль за уровнем защищенности информации, содержащейся в информсистемах.

Весьма важным вопросом, связанным с защитой информационных систем в ГИМУ, является вопрос по безопасности взаимодействия пользователей систем при их идентификации (аутентификации), что предполагает корректную настройку протоколов и взаимодействий, а также прав доступа. Могут использоваться электронные подписи[16].

Таким образом, можно говорить о достаточно стройной системе законодательства по обеспечению информационной безопасности в Российской Федерации и достаточно четком распределении обязанностей по ее обеспечению между федеральными структурами. Стоит отметить,

[15] Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (с изм. и доп., вступ. в силу с 01.01.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_147084/ (режим доступа 1.02.2021).

[16] Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (режим доступа 1.02.2021).

что поддержание информационной безопасности в ГИМУ на высоком уровне влечет за собой большие материальные затраты. Однако защита информации, в том числе персональных данных, является одной из первостепенных задач и должна быть обеспечена в соответствии с действующим законодательством Российской Федерации.

Использованные источники:

1. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (режим доступа 1.02.2021).

2. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_6300/ (режим доступа 1.02.2021).

3. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (режим доступа 1.02.2021).

4. Указ Президента РФ от 11.08.2003 N 960 (ред. от 03.07.2018) "Вопросы Федеральной службы безопасности Российской Федерации" // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_43763/ (режим доступа 1.02.2021).

5. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 31.08.2020) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_14031/ (режим доступа 1.02.2021).

6. Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 30.01.2021) "О Министерстве цифрового развития, связи и массовых

коммуникаций Российской Федерации"// Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_77387/ (режим доступа 1.02.2021).
7. Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.12.2020) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_85889/ (режим доступа 1.02.2021).
8. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 16.12.2020) "Об утверждении государственной программы Российской Федерации "Информационное общество" (с изм. и доп., вступ. в силу с 26.12.2020) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_162184/42f381c81a151303511bc36ecea815d2fb3050fe/ (режим доступа 1.02.2021).
9. Приказ ФСТЭК России от 12.05.2005 N 167 (ред. от 26.04.2018) "Об утверждении Регламента Федеральной службы по техническому и экспортному контролю" (Зарегистрировано в Минюсте России 06.06.2005 N 6682) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_53859/ (режим доступа 1.02.2021).
10. Приказ ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (с изм. и доп., вступ. в силу с 01.01.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_147084/ (режим доступа 1.02.2021).

11. Приоритетные направления поддержки проектов по разработке и внедрению отечественного программного обеспечения в рамках сквозных цифровых технологий (высокотехнологичных направлений) в 2020 году (утверждены протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27 августа 2020 г. №17). URL: https://digital.gov.ru/uploaded/files/prioritetnyie-napravleniya-podderzhki-proektov-po-razrabotke-i-vnedreniyu-otechestvennogo-programmnogo-obespecheniya-v-ramkah-skvoznyih-tsifrovyih-tehnologij-vyisokotehnologichnyih-napravlenij-v-2020-godu.pdf (режим доступа 1.02.2021).

12. Аксенов С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Безопасность бизнеса. - М.: Юрист, 2008, № 3. С. 5-10

13. Васильев В.Н., Парфенов В.Г. Подготовка высококвалифицированных специалистов в области разработки программного обеспечения // Компьютерные инструменты в образовании. №1. 2012. С.48-56.

14. Николай Никифоров выступил на Гайдаровском форуме // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Официальный сайт. URL: https://digital.gov.ru/ru/events/34523/ (режим доступа 1.02.2021).

15. Остапенко В.С. Информационная безопасность региональных органов исполнительной власти // Государственное и муниципальное управление. Ученые записки СКАГС. - Р-н/Д: СКАГС, 2009. С.160-169.

16. Справочная информация: "Структура и функции федеральных органов исполнительной власти и управления" (Материал подготовлен специалистами КонсультантПлюс). URL: http://www.consultant.ru/document/cons_doc_LAW_120971/ (режим доступа

1.02.2021).