Антошин В. А. – канд. филос. наук, профессор
e-mail: valeryiantoshin@yandex.ru
Швецова Л. А.
e-mail: lshvetsova_a@icloud.com

Обеспечение информационной безопасности как важнейшая функция государственного управления

Актуальность темы исследования. Современный мир живет в реалиях информационного общества, в котором информация является основным способом взаимодействия людей и развития экономики. Это в полной мере относится и к России, где вопросы информационной безопасности актуализированы в Указе Президента от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» [3]. Наличие этого Указа, а также Доктрины информационной безопасности Российской Федерации, утверждённой Указом Президента РФ № 646 от 05.12.2016 свидетельствует о понимании государственной властью важной роли информации, ее безопасном хранении, передаче и обработке.

Также нужно отметить статистику незаконного разглашения персональных данных – основную угрозу информационной безопасности. В целом по России за 2022 год было опубликовано 667 миллионов учётных записей по данным InfoWatch [29]. За 2023 год, по данным Роскомнадзора, были опубликованы только 300 миллионов учётных записей через 168 инцидентов, а в 2024 уже 500 миллионов [30]. Неизбежно инциденты случаются и у государственных органов, например, за 2019 год СМИ сообщали о разглашении персональных данных пользователей Госуслуг (около 30 тысяч учётных записей) [31].

Степень разработанности темы. Следует выделить авторов по информационной безопасности, которые многие свои работы посвятили данной теме, некоторые из них выступили научными редакторами учебников для бакалавров: Т. А. Полякова, А. А. Стрельцова; И. Л. Морозов; И. Л. Бачило, В. Н. Лопатин, М. А. Федотов, Б. Н. Топорнин; В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков. Кроме них, данной темой занимались: И. М. Рассолов, П. У. Кузнецов, М. А. Ефремова, исследовавшие правовую сторону информационной безопасности и возможных мер ответственности для её нарушителей. Принципы информационной безопасности исследует среди прочих Ю. Е. Кулавская. Также можно выделить Л. К. Терещенко, О. И. Тиунова, которые исследовали информационную безопасность в контексте деятельности исполнительных органов власти.

Таким образом, можно заключить, что тема активно изучается, но в силу динамичности исследуемого объекта (информации) и способов её использования, исследования необходимо продолжать.

Объект исследования – информационная безопасность как важнейшая функция государственного управления.

Предмет исследования – анализ информационной безопасности в контексте ее принципов и некоторых направлений деятельности органов государственной власти по ее обеспечению.

Цель исследования – на основе анализа нормативно-правовых актов, исследований специалистов в области информационной безопасности, а также сложившихся фактических условий в сфере информационной безопасности, **выявить основные тенденции**

государственного управления в сфере информационной безопасности как важнейшей функции обеспечения безопасности государства.

Исследуемой **управленческой проблемой** является обеспечение информационной безопасности общества и государства в рамках деятельности органов государственной власти.

В процессе написания данного исследования использованы следующие **общенаучные методы** познания: анализ, индукция, обобщение, сравнительный метод.

Авторский анализ. Концепция безопасности и непосредственно ее обеспечения является одной из ключевых ценностей для каждого государства, которую оно, при условии, что не является «несостоявшимся» (failed state) [14], стремится поддерживать и обеспечивать в той мере, в которой это представляется возможным. Какую бы функцию государства мы не рассматривали – будь то экономическая, социальная и т.д. – везде красной нитью проходит идея обеспечения безопасности. Согласно О.А. Белькову [11], безопасность представляется состояние развития общества, которое позволяет ему полноценно функционировать, что, по сути, говорит о необходимости безопасности для дальнейшего развития государства. Применительно к России, более глобально эта идея сформулирована в понятии «национальная безопасность» [5] – комплексной концепции, относящейся к защите национальных интересов Российской Федерации от внешних и внутренних угроз, которая гарантирует реализацию конституционных прав и свобод граждан, обеспечивает достойное качество жизни и уровень благосостояния населения, поддерживает гражданский мир и согласие в стране и, кроме того, направлена на защиту суверенитета страны, ее независимости и единства, а также на обеспечение устойчивого социально-экономического прогресса.

В современных условиях, когда цифровизация стала актуальной общемировой повесткой и начала захватывать всё больше сфер жизни людей, мы очень часто обращаем внимание на проблемы информационной безопасности, защиты информации в контексте национальной безопасности.

Согласно словарю русского языка С. И. Ожегова, информация – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством [25]. А согласно п. 1 ст. 2 ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», «информация - сведения (сообщения, данные) независимо от формы их представления» [2].

В виду того, что информация о происходящих событиях разными субъектами может формулироваться по-разному, она становится достаточно мощным рычагом влияния на конкретный объект. Другими словами, информация является манипулятивной концепцией и может трактоваться разными субъектами по-разному в зависимости от их целей. Очевидно, что манипулированию посредством информации могут быть подвержены не только отдельные люди, но целые страны. И это осознание неизбежно приводит государство к необходимости обеспечить свою безопасность и оградить своих граждан от той информации, которая потенциально способна нанести вред. Так, в числе основных положений концепции национальной безопасности многих государств, в ряду которых Российская Федерация не является исключением, начала фигурировать и «безопасность информационного пространства» [1]. В связи с этим, в нормативно-правовой литературе зафиксировано определение этого понятия, отсутствие чего сделало бы невозможным какое-либо регламентирование и нормативное регулирование в данном вопросе.

Согласно Доктрине информационной безопасности Российской Федерации, определение понятия «информационная безопасность» практически полностью дублирует содержание понятия «национальная безопасность» из вышеприведённой Стратегии [4]. Можно предположить, что это связано с пониманием российским законодателем ключевых свойств информации, а также того, что информация пронизывает все сферы общества и обеспечение национальной безопасности в полной мере возможно только в случае реализации информационной безопасности.

Обращаясь к другим трактовкам понятия «информационная безопасность», мы видим, что существует достаточно большое количество различных подходов для рассмотрения данной категории. В своей статье Н. А. Северцев и А. А. Бецков [19] определяют информационную безопасность как состояние защищенности информационной среды национальной безопасности, обеспечение формирования, использования и развития в интересах человека, общества и государства. В. Н. Ясенев в своем учебнике определяет информационную безопасность как невозможность причинения вреда свойствам объекта безопасности, которые обусловлены информацией и информационной инфраструктурой [24]. Сравнивая эти определения, мы видим, что специалисты в целом сходятся во мнении по поводу сущности данного понятия. По нашему мнению, это объясняется тем, что понятие информационной безопасности – достаточно устоявшееся как в теории, так и в практике, что обусловлено ее связью с одной из основных сфер национальной безопасности.

Таким образом, мы можем констатировать, что понятие информационной безопасности, необходимое для рационального построения соответствующей политики, в нормативно-правовых актах используется достаточно последовательно, а в научной дискуссии не вызывает особенных споров, что является хорошим признаком проработанности данной темы.

Прежде всего, следует обратить внимание на те вызовы, с которыми потенциально сталкивается государство при обеспечении информационной безопасности. Во-первых, исходя из выделенной в Стратегии национальной безопасности Российской Федерации цели обеспечения информационной безопасности, которая заключена в сохранении суверенитета России в информационном поле, мы можем обратить внимание на попытки как иностранных, так и отечественных лиц, группировок и организаций вмешаться в политическую, экономическую и иные сферы деятельности государства [5]. Во-вторых, цифровизация дала субъектам, занимающимся терроризмом и/или экстремизмом, новый инструмент для реализации их деятельности – Интернет, который позволил им расширить сферу деятельности, а также упростить в некоторых вопросах реализацию актов экстремизма и терроризма [5]. В-третьих, какой бы эффективной не была Стратегия обеспечения информационной безопасности, всегда надо учитывать человеческий фактор [13]. Киберпреступники предпринимают попытки социального инжиниринга для достижения собственных целей: отправляют работникам компании или госоргана на электронную почту сообщения, содержащие вирусы, распространяют вредоносное программное обеспечение в расчете на то, что его по ошибке установят, входят в доверие к сотрудникам организаций и добывают информацию таким образом, и т.д. [23] Часть исследователей выделяет следующие принципы информационной безопасности:

- конфиденциональность;
- целостность;
- доступность [12].

Конфиденциальность информации означает, что доступ к ней должен быть только у тех, кто обладает правом на доступ. В частности, доступ к аккаунту на госуслугах должен быть только у человека, с чьей личностью он связан. Доступ к информации, связанной с государственной тайной только у людей, которые подписали соглашение о неразглашении государственной тайны и т.д. Само собой, что есть информация, для которой не требуется особая проверка личности запрашивающего информацию, поскольку информация является публичной, предназначенной для широкого доступа. В этом случае подразумевается, что такая информация должна быть опубликована на общедоступном, не требующем регистрации сайте (Постановления Правительства РФ на сайте правительства РФ, например).

Целостность информационной безопасности означает, что вносить изменения в информацию могут лишь лица, обладающие правом на доступ к ней, то есть изменять данные паспорта (по достижении 20 лет) в аккаунте на госуслугах должен лишь человек, с чьей личностью связан данный аккаунт.

Доступность информации означает непрерывный доступ информации лицам, обладающим правом на её получение. У этого принципа есть два аспекта: информация должна быть доступна непрерывно и информация не должна быть утеряна в результате ошибок людей, обслуживающих информационную систему или хакерских атак. Это придаёт такую большую роль резервному копированию данных.

Другая часть исследователей выделяет другие принципы информационной безопасности [15]. Если приведённые выше принципы можно назвать описывающими необходимые свойства системы информационной безопасности, то к принципам построения такой системы относятся:

- наименьшей привилегии;
- разделения обязанностей;
- глубокой защиты;
- безопасного отказа;
- открытого проектирования;
- минимизации площади поверхности атаки [15].

Принцип наименьшей привилегии связан с тем, что так или иначе части пользователей приходится предоставлять достаточно широкие права (например, управляющим компанией или HR-специалистам, добавляющим и удаляющим из базы данных сотрудников государственного органа). В этом случае не следует давать неограниченный доступ ко всем информационным ресурсам сервера, а лишь к той части, что обуславливает функцию сотрудника, получающего доступ. Так, тот же HR-специалист не должен получать доступ к аккаунтам сотрудников в информационной системе, если всё, что ему необходимо от неё – добавлять новых и удалять уволенных сотрудников.

Принцип разделения обязанностей связан с принципом наименьшей привилегии, но всё же отличается от неё. Если первый принцип предполагает необходимость следить за техническим ограничением прав больше необходимого, то принцип разделения обязанностей должен учитываться ещё при создании (изменении) структуры государственного органа и распределении обязанностей. Так сотрудник, который ответственен за приём и консультирование посетителей, не должен иметь доступа к принятию решений о предоставлении или непредоставлении права конкретному посетителю на приём, так как здесь возникает риск злоупотребления правом в личных интересах.

Принцип глубокой защиты означает, что в случае несанкционированного проникновения в систему, должен быть реализован сценарий, который позволит пресечь

такое проникновение. В результате злоумышленник не получит информацию больше той, что успел сохранить. Например, в таком сценарии может быть реализована блокировка сервера для взаимодействия с иными устройствами или стирание всех данных.

Принцип безопасного отказа специалисты выделяют, из понимания, что система защиты рано или поздно потерпит неудачу и необходимо минимизировать последствия атаки. Для этого следует предпринимать профилактические действия, вроде сохранения резервных копий состояния системы. И таким образом мы также дополняем реализацию вышеназванного принципа – принципа доступности.

Принцип открытого проектирования означает, что безопасность должна достигаться не за счёт запутанности, неизвестности информации об архитектуре системы, а за счёт математической/технической сложности взлома системы. Прекрасным примером реализации является RSA-шифрование [21].

И, наконец, принцип минимизации площади поверхности атаки означает, что у системы должно быть как можно меньше потенциально уязвимых мест, которыми могут воспользоваться злоумышленники. То есть если что-то можно не делать вовсе – предпочтительнее не делать, во избежание совершения ошибок при проектировании.

И как определенный вывод в характеристике системы принципов хотелось бы привести высказывание Б. Шнайера, иностранного специалиста по информационной безопасности: «Система безопасности надежна настолько, насколько надежно ее самое слабое звено» [22]. Это означает, что при проектировании системы безопасности, неважно, маленькой компании или государственного органа, занимающегося международной слежкой, нельзя бесконечно делать упор на отдельные части системы и забывать про другие. Например, нет никакого смысла в совершенном алгоритме шифрования, если компьютер каждого сотрудника государственного органа имеет доступ ко всем файлам организации.

По нашему мнению, вышеприведённые принципы являются общими для любой системы информационной безопасности, неважно, коммерческая это организация или государственная система предоставления государственных услуг на основе авторизации граждан с хранением их конфиденциальной информации. Дальше мы рассмотрим, какими принципами дополняются системы информационной безопасности в государственных органах.

Рассматривая информационную безопасность в государственных органах, стоит начать с того, что качество государственного управления в сфере информационной безопасности является критически важным для обеспечения безопасности страны в современном информационном обществе. От данной политики государства зависит, например, насколько будут защищены конфиденциальные данные граждан, то есть, по сути, насколько будет защищено в его стране конституционное право граждан на частную жизнь. Степень защищённости в этой сфере называется информационной безопасностью.

В. Н. Лопатин в своей работе дал определение информационной безопасности Российской Федерации: это такое состояние защищённости в информационной сфере, которое удовлетворяет потребности человека и общества, даёт возможности для устойчивого развития [16].

Важно отметить, что это не состояние защищённости информации, а состояние защищённости субъектов – человека и общества, определяемое через их защищённость в информационной среде.

Государственное регулирование в области обеспечения информационной безопасности основано на законодательстве Российской Федерации, и осуществляется путём

внесения, изменения или исключения из него соответствующих нормативно-правовых актов [18]. При этом следует заметить, что из-за общих процессов развития современного права России регулирование осуществляется за счёт широкого спектра отраслей, переплетающихся друг с другом, а не выделяется в какую-то отдельную отрасль [9], хотя и некоторые авторы говорят о так называемом «суперинституте» [10] информационного права.

При этом, если мы рассматриваем государственное управление в сфере обеспечения информационной безопасности, то она включает в себя государственное регулирование, как часть субъект-объектных отношений между наделёнными и ненадёленными властью акторами, в сфере отношений по созданию, передаче и использованию информации [17]. Таким образом, государственное регулирование обеспечения информационной безопасности является лишь инструментом для всей сферы государственного управления обеспечением информационной безопасности, входит в государственное управление как подмножество.

В рамках ст. 16 ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», выделяются следующие направления защиты информации на государственном уровне:

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации» [2].

Нужно учитывать, что эти направления касаются информации как таковой, распространяющейся через Интернет. Речь в данном случае об информации, подлежащей конфиденциальности (например, переписки пользователей, хранящиеся в социальных сетях и распространяемые через интернет). Так, 16 статья ФЗ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2] упоминается в деле о нарушении права на переписку сотрудником спецслужб при превышении своих полномочий [7]. Такие дела завязаны также на законы «О персональных данных», «О связи», затрагивают несколько статей Конституции РФ, касающихся прав и свобод граждан в частной жизни [1].

Также защите подлежит свобода распространения информации, то есть государство гарантирует здесь пресечение попыток помешать свободному распространению информации и деятельности СМИ через интернет при неправомерном доступе к информации [8].

При этом в обеспечение информационной безопасности самих государственных органов входят:

- обеспечение органов и граждан, взаимодействующих с ними, необходимой информацией, а главное в данном контексте – своевременной, точной и соблюдающей принцип конфиденциальности;
- обеспечение безопасности хранящейся информации;
- обеспечение безопасной передачи информации [20].

На мой взгляд, такое выделение элементов позволяет полностью охватить структуру обеспечения информационной безопасности, позволяя при этом выделять отдельные области для дальнейшего изучения и углубления познания.

Для выделения цели данной деятельности можно обратиться к концепции информационной безопасности ФНС России, в которой говорится, что целью является защита законных права граждан и юридических лиц; защита информации, подлежащей защите (например, государственная тайна); защищённость информационных систем [3].

В этой же концепции приводятся следующие принципы обеспечения информационной безопасности:

1. принцип законности;
2. принцип системности и комплексности;
3. принцип максимальной дружественности;
4. принцип превентивности;
5. принцип адекватности и непрерывности;
6. принцип адаптивности;
7. принцип доказательности и своевременности контроля;
8. принцип самозащиты и конфиденциальности;
9. принцип нескольких уровней защиты;
10. принцип простоты применения;
11. принцип преемственности и совершенствования;
12. принцип персональной ответственности и минимизации прав;
13. принцип разделения обязанностей;
14. принцип разумной достаточности;
15. принцип централизации [3].

Сравнив их с принципами выше, можно заключить, что список принципов, закреплённый в нормативных актах, гораздо шире, чем список принципов, выделяемый экспертами. В частности, к спискам принципов выше добавляются принципы законности, максимальной дружественности, превентивности, адекватности и непрерывности, доказательности и своевременности контроля, простоты применения, централизации [3].

Принцип законности выделяется, поскольку любая деятельность государственных органов основывается на законах.

Принцип максимальной дружественности означает желательное соответствие технологий, применяемых для обеспечения информационной безопасности, технологиям, уже применяемым в ФНС России.

Принцип превентивности означает предотвращение угроз до их возникновения.

Принцип адекватности и непрерывности выражает идею распределения ресурсов по обеспечению информационной безопасности в соответствии с ценностью и конфиденциальностью информации, а также на протяжении всего срока жизни объектов информатизации.

Принцип доказательности и своевременности контроля означает, что информация должна проверяться на подлинность с помощью соответствующих технических средств, а любое нарушение безопасности должно сразу фиксироваться.

Принцип простоты применения касается человеческого фактора в системе безопасности, в частности, любое средство безопасности (введение логина и пароля, двухфакторная аутентификация и т.д.) должно быть интуитивно понятно пользователю, пользователь должен осознавать, для чего эта мера существует. Также необходимо избегать действий, которые вызывают значительные трудозатраты пользователя на взаимодействие с системой.

Принцип централизации означает, что за счёт применения технологий решение задач должно осуществляться минимально возможным количеством людей, полномочия которых должны быть предельно чёткими и ясными.

Может возникнуть ощущение, что принципы, выделенные в данном нормативно-правовом акте, слегка избыточны. Однако если эти правила построения системы были

выделены в отдельные принципы, то почти наверняка их неприменение стало брешью в системе безопасности, причём не единожды.

Необходимо отметить, что возможные последствия отличаются в случае утечки данных, намеренных хакерских атак или ненамеренных сбоев в системе / стирания данных. Так, к примеру, на портале госуслуги зарегистрировано на данный момент практически 100 миллионов записей (каждый гражданин РФ может зарегистрировать лишь одну запись), что составляет более 2/3 всего населения России [26]. В случае если злоумышленник сможет взломать базу данных портала или получить доступ к любому аккаунту таким образом, чтобы система ничего не заподозрила – под угрозой окажется огромный массив либо конфиденциальных данных, либо волеизъявление граждан, совершаемое через Интернет, в частности, через портал «Госуслуги». Учитывая, какое огромное количество услуг ежедневно предоставляется гражданам (в данный момент за 2023 год прогнозируется предоставление более 500 миллионов услуг) [26], то если будет обнаружена такая уязвимость, очень большое количество граждан не сможет своевременно воспользоваться государственными услугами и решить какие-либо свои, порой очень срочные и важные, вопросы. Косвенный ущерб для экономики в таком случае может исчисляться миллионами, а может и миллиардами, в зависимости от того, насколько сложна и глубока окажется уязвимость портала.

Интересно также сравнить информационную безопасность в государственных органах и бизнесе.

Согласно глобальному исследованию Search Inform за 2021 год, меньше половины компаний в России внедряют у себя серьёзные средства защиты от кибератак, часть ограничиваются только антивирусом [27].

Согласно же исследованию Positive Technologies, на госучреждения приходится 25 % всех зарегистрированных атак, остальные 75 % процентов приходятся на негосударственные компании [28].

К сожалению, данные статистики можно трактовать совсем по-разному – либо в государственных органах лучше безопасность при одинаковом с частным сектором количестве атак, либо в государственных органах не развиты средства отслеживания атак, что повлияло на статистику, либо же просто государственные органы гораздо менее интересны злоумышленникам.

Также нет никакой чёткой статистики по тому, какое операционное обеспечение применяется в органах государственной власти. Более того, даже сайты «визитки» каждого органа могут отличаться от других органов. Допустим, сайт визитка министерства социальной политики Свердловской области (https://msp.midural.ru) легко может отличаться от министерства финансов всё той же Свердловской области (https://minfin.midural.ru). Это говорит о том, что реализация требований о предоставлении информации для граждан никак не урегулирована с технической точки зрения. Нет единого исполнителя сайтов (и скорее всего, единого исполнителя информационной безопасности) для всех государственных органов.

По нашему мнению, в этом смысле государственные органы гораздо больше похожи на малые и средние компании. Есть и свой «Яндекс» – «Портал государственных услуг», над которым работало очень много специалистов, как над работоспособностью сайта, так и над его дизайном, так и над его безопасностью, и который показывает очень хорошие результаты своей работы; есть и свои малые и средние предприятия – это сайты министерств, отделов различных субъектов РФ.

Таким образом, между информационным обеспечением государственных органов и информационным обеспечением бизнеса не так уж много отличий. Они строятся на схожих принципах, они одинаково подвергаются атакам, имеют общие проблемы (согласно статистике). Сложно сказать, в утечке данных откуда больше риска – если речь идёт о Портале государственных услуг или о Яндексе (и его сервисах) – то персональные данные большого количества граждан будут нарушены в случае кражи баз данных. Если же речь идёт о каком-то малом предприятии или государственном органе, которые могли даже не собирать персональные данные через интернет — то максимальный ущерб может быть нанесён путём дестабилизации их деятельности.

В целом, подводя итог исследованию, нужно подчеркнуть, что информационная безопасность является достаточно разработанной категорией с теоретической точки зрения, но на практике её часто недооценивают, особенно там, где нет большой концентрации персональных данных. На наш взгляд, нужна серьезная работа по совершенствованию в сфере реализации основных принципов защиты информации в органах государственного управления.

Литература:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изм., одобренными в ходе общероссийского голосования 01.07.2020) // СПС КонсультантПлюс.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СПС КонсультантПлюс.

3. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СПС КонсультантПлюс.

4. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС КонсультантПлюс.

5. Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации» // СПС КонсультантПлюс.

6. Приказ ФНС России от 06.04.2021 N ЕД-7-24/298@ «О внесении изменений в Концепцию информационной безопасности Федеральной налоговой службы» // СПС КонсультантПлюс.

7. Постановление Шуйского городского суда Ивановской области от 22.01.2024 по делу N 1-25/2024 (1-255/2023) // СПС КонсультантПлюс.

8. Приговор Советского районного суда города Тулы от 13.10.2023 N 1-139/2023 // СПС КонсультантПлюс.

9. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право: учебник / под ред. Б. Н. Топорнина. – СПб.: Юридический центр Пресс, 2001. – 789 с.

10. Бачило И. Л. О подходах к систематизации и кодификации информационного законодательства // Систематизация и кодификация информационного законодательства: сб. научных работ / отв. ред. И. Л. Бачило. – М.: Изд-во ИГП РАН, 2015. – 216 с.

11. Бельков О.А. Понятийно-категориальный аппарат концепции национальной безопасности // Безопасность. 1994. № 3. – 4 с.

12. Какорин И. А. Основные принципы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2023. № 2-2 (77). – С. 25-27.

13. Капустин Ф. А. Информационная безопасность и защита информации в современном обществе // Актуальные проблемы авиации и космонавтики. 2016. №12. – С. 738-740.

14. Кравцова А. А. Переход от состояния «несостоявшегося государства» (failed state) к распаду государства: сравнительный анализ // Выпускные квалификационные работы студентов НИУ ВШЭ. – 2014. – 81 с.

15. Кулавская Ю. Е. Принципы обеспечения информационной безопасности // E-Scio. 2021. № 5 (56). – 5 с.

16. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. – М., 2000. – 428 с.

17. Морозов И. Л. Государственное управление в сфере информационной безопасности современной России: учебно-методическое пособие. – Волгоград: Изд-во Волгоградского института управления – филиала РАНХиГС, 2021. – 88 с.

18. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под ред. Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2023. – 357 с.

19. Северцев Н. А., Бецков А. В. Информационная безопасность и принципы ее обеспечения // НиКа. 2018. № 1. – С. 92-96.

20. Терещенко Л. К., Тиунов О. И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. №8 (224). – С. 100-109.

21. Шемет В. С., Айдинян А. Р. Обзор методов шифрования // Символ науки. 2016. № 6-1. – С. 112-115.

22. Шнайер Б. Практическая криптография / Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 432 с.

23. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). – С. 133-138.

24. Ясенев В. Н., Дорожкин А. В., Сочков А. Л., Ясенев О. В. Информационная безопасность: учеб. Пособие, под общ. ред. В.Н. Ясенева. – Нижний Новгород: Нижегородский гос. ун-т им. Н.И. Лобачевского, 2017. – 198 с.

25. Толковый словарь Ожегова [Электр. ресурс]. URL: https://slovarozheg*ova.ru/word.php?wordid=10048 (дата обращения: 31.09.2024).

26. Новости национального проекта «Цифровая экономика» [Электр. ресурс]. URL: https://национальныепроекты.рф/news/kolichestvo-uchetnykh-zapisey-na-portale-gosuslug-v-2022-godu-dostiglo-99-mln (дата обращения: 31.09.2024).

27. Глобальное исследование Search Inform [Электр. ресурс]. URL: https://searchinform.ru/survey/global-2021/ (дата обращения: 31.09.2024).

28. Исследование Positive Technologies [Электр. ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/outcomes-of-IS-incident-investigations-in-2021-2023-years/ (дата обращения: 31.09.2024).

29. InfoWatch сообщила о росте в РФ объема утечек в 2,7 раза, до 667 млн записей [Электр. ресурс] // Коммерсантъ. URL: https://www.kommersant.ru/doc/5939235 [дата обращения: 31.09.2024].

30. В результате крупного инцидента в 2024 году в сеть утекли 500 млн записей о россиянах [Электр. ресурс] // ТАСС. URL: https://tass.ru/obschestvo/20065237 (дата обращения: 31.09.2024).

31. СМИ узнали об утечке данных пользователей сайта госуслуг [Электр. ресурс] // РБК. URL: https://www.rbc.ru/society/29/12/2019/5e08a43d9a7947345490f23e (дата обращения: 31.09.2024).