УДК 004.056 **DOI: 10.34670/AR.2020.76.82.048**

Проблемы обеспечения информационной безопасности в системе МВД России при работе с базами данных

Ефремов Александр Филиппович

Слушатель
Академия управления МВД России,
125171, Российская Федерация, Москва, ул. Зои и Александра Космодемьянских, 8;
e-mail: postvim@mail.ru

Аннотация

Сегодня глобальная цифровизация охватывает весь мир, влияя не только на жизнь общества, но и на функционирование органов государственной власти, при этом МВД России не является тому исключением. Так, за последние несколько лет МВД России включило в свои основные процессы и системы управления облачные технологии, большие данные, интернет, искусственный интеллект, которые, в свою очередь, позволили эффективно систематизировать и консолидировать большие объемы информации, содержащиеся в разрозненных аналоговых базах данных, в единые информационные цифровые базы данных. Такие информационные цифровые базы данных во много раз увеличили эффективность работы МВД России в его основной сфере деятельности - обеспечении общественной безопасности и противодействии преступности.

Тем не менее, при внедрении в деятельность МВД России цифровых технологий появились проблемы, связанные с обеспечением информационной безопасности. Анализ деятельности МВД России в части работы с базами данных позволил прийти к выводу о том, что в данном ведомстве существует две группы проблем обеспечения информационной безопасности. Первая группа проблем — это проблемы надлежащей организации обеспечения безопасности. Такие проблемы первичны, и их наличие порождает вторичные проблемы – проблемы обеспечения информационной безопасности, связанные непосредственно с работой в базах данных: несанкционированный доступ к информации, ее хищение, а также искажение данных, вносимых в базы данных. Решить такие проблемы возможно за счет проведения комплекса мероприятий, направленных на обеспечение информационной безопасности, начиная с правильно организованного обучения информационной безопасности и заканчивая внедрением новых технологий в системы контроля.

Для цитирования в научных исследованиях

Ефремов А.Ф. Проблемы обеспечения информационной безопасности в системе МВД России при работе с базами данных // Вопросы российского и международного права. 2020. Том 10. № 11А. С. 229-235. DOI: 10.34670/AR.2020.76.82.048

Ключевые слова

Базы данных МВД России, обеспечение информационной безопасности, несанкционированный доступ к информации, хищение информации, системы контроля доступа к информации, искажение данных.

Введение

Сегодня в основе эффективного функционирования органов государственной власти лежит использование цифровых технологий, и Министерство внутренних дел Российской Федерации (далее – МВД России) не является тому исключением. Вместе с тем использование цифровых технологий в деятельности органов государственной власти предоставляет не только преимущество, но и несет в себе существенную угрозу, особенно в тех областях, которые связаны с использованием цифровых технологий для получения и обработки информации, которая, в соответствии с законодательством Российской Федерации, не является общедоступной. Применительно к системе МВД России такой информацией можно назвать любую информацию, содержащуюся в различных единых цифровых базах данных. Сказанное позволяет вывести на первый план при работе с едиными цифровыми базами данных МВД России группу проблем, связанных с информационной безопасностью.

Однако, прежде чем акцентировать внимание непосредственно на проблемах обеспечения информационной безопасности при работе с базами данных МВД России и определить возможность минимизации таких проблем, необходимо понять, что именно охватывается категориями «информационная безопасность» и «обеспечение информационной безопасности».

Основное содержание

Основы обеспечения информационной безопасности в масштабах страны заложены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации №646 от 5 декабря 2016 года (далее – Доктрина ИБ). В соответствии с положениями названного документа, информационная безопасность есть состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие страны, оборона страны и ее безопасность.

Обеспечением информационной безопасности, в соответствии с Доктриной ИБ, признается осуществление взаимоувязанных мер (правового, организационного, оперативно-разыскного, научно-технического и иного характера), направленных на прогнозирование, обнаружение, сдерживание, предотвращение, отражение информационных угроз и ликвидацию последствий их проявления.

Таким образом, Доктрина ИБ связывает информационную безопасность и ее обеспечение с необходимостью защиты соответствующих субъектов и информации о таких субъектах и действиями, направленными на осуществление такой защиты. При этом обеспечение информационной безопасности можно охарактеризовать как комплекс действий, включающих в себя не только защиту самой информации в части обеспечения ее конфиденциальности, целостности и доступности, но и защиту информационной инфраструктуры, криптографии, реагирование на инциденты, управление уязвимостями и аварийное восстановление.

В специализированной литературе информационную безопасность обычно связывают с параметрами защищенности информационного пространства от воздействия неблагоприятных факторов и условий [Артамонова, 2008; Бирюков, 2018; Кемпф, 2019], в основе которой лежит три ключевых элемента – конфиденциальность, целостность и доступность [Плахина, 2019;

Ребрий, 2020]. Если какой-либо из этих трех элементов будет скомпрометирован, это может привести к серьезным последствиям как для того, кто уполномочен на контроль данных данных, так и для отдельных лиц, данные о которых подлежат обработке. Обеспечение же информационной безопасности в первую очередь связано с необходимостью осуществления комплекса мероприятий, направленных на достижение защищенности информационного пространства [Сухаренко, 2018].

В контексте настоящей статьи правильнее было бы придерживаться того подхода к обеспечению информационной безопасности, который закреплен законодательно, поскольку он наиболее полно и точно раскрывает перечень тех мер, которые должны быть направлены на обеспечение информационной безопасности, а соответственно позволяет более детально проработать направления минимизации проблем обеспечения информационной безопасности в пределах конкретной системы. Кроме того, указание на Доктрину ИБ как на основу обеспечения информационной безопасности в системе МВД России содержится во всех локальных актах МВД России, связанных с работой с информацией и базами данных, среди которых Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (далее – Концепция ИБ МВД), утвержденная Приказом МВД России от 14.03.2012 №169, а также Приказ МВД России от 23.11.2016 № 755 «Вопросы эксплуатации центра разработки, поддержки, внедрения и администрирования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России». При этом саму информационную безопасность будем рассматривать исходя из классической триады – конфиденциальность, целостность и доступность, поскольку любые меры обеспечения информационной безопасности всегда направлены на то, чтобы гарантировать наличие всех трех обозначенных элементов как для самих баз данных, так и для любых данных, которые они обрабатывают.

Проблемы обеспечения информационной безопасности всегда вытекают из того, что ненадлежащим образом выполняются задачи, направленные на обеспечение такой информации. Исходя из раздела IV Концепции ИБ МВД, задачи по обеспечению информационной безопасности в системе МВД России сводятся к предотвращению утечки, хищения, утраты информации, неправомерных действий по ее уничтожению, модификации, искажению, несанкционированному копированию и блокированию, обеспечению конфиденциальности информации и защите персональных данных путем применения организационных и технических мер в соответствии с законодательном Российской Федерации в рамках подсистемы обеспечения информационной безопасности Информационной системы обеспечения деятельности МВД России (далее – ИСОД МВД).

Так, исходя из содержания протокола совещания последней коллегии МВД России, посвященной развитию информационных систем в системе МВД России, состоявшейся 5 декабря 2018 года, можно сделать вывод о том, что ненадлежащим образом выполняются такие задачи обеспечения информационной безопасности, как: предотвращение утечек, хищение информации, предотвращение искажения информации и ее несанкционированное копирование. Так, в Решении вышеназванной коллегии, в частности отражено, что в МВД России проблемы возникают в части предупреждения, выявления и пресечения незаконного доступа к информационным ресурсам, банкам данных, оперативно-справочным, профилактическим и розыскным учетам системы МВД России, в том числе со стороны уволенных или освобожденных от занимаемых должностей сотрудников органов внутренних дел, собирающих информацию из баз данных в целях неправомерного использования (распространения). Кроме того, не решена и проблема предупреждения, выявления и пресечения умышленного искажения

данных, загружаемых в информационные ресурсы, банки данных, оперативно-справочные, профилактические и розыскные учеты системы МВД России.

Угрозы информационной безопасности, по мнению автора настоящей статьи, почти всегда носят комплексный характер, поэтому утечки, хищения информации, а равно ее искажение и несанкционированное копирование в рамках одной базы данных могут повлиять на эффективность деятельности МВД России в целом. Поэтому МВД России должно не просто давать указание соответствующим территориальным органам о необходимости предупреждения, выявления и пресечения незаконного рода угроз информационной безопасности в части работы с базами данных, но и принимать активное участие при реализации территориальными органами соответствующих мероприятий, обеспечив надлежащий уровень контроля за мероприятиями по обеспечению информационной безопасности со стороны сиротствующих департаментов, управлений и подведомственных учреждений.

Кроме того, видится необходимым и разработка со стороны МВД России более действенных мер, направленных на предотвращение угроз информационной безопасности за счет более тщательной подготовки специалистов как в сфере информационной безопасности, так и лиц, деятельность которых в будущем будет связана с работами с базами данных МВД России. Как отмечается в специализированной литературе, в настоящий момент времени в системе МВД России специалистов с нужными знаниями и навыками в сфере обеспечения информационной безопасности недостаточно [Кемпф, 2019; Кубасов, 2020]. Именно поэтому необходимо разработать комплекс мероприятий в части подхода к обучению курсантов и слушателей ведомственных вузов, направленных не на формальное обучение, а на стимулирование и развитие у курсантов и слушателей навыков кибербезопасности.

Вышеназванные проблемы можно назвать проблемами надлежащей организации обеспечения безопасности. Такие проблемы являются, на наш взгляд первичными, и их наличие порождает вторичные проблемы – проблемы обеспечения информационной безопасности, связанные непосредственно с работой в базах данных, когда речь идет о несанкционированном доступе к информации, ее хищении, а также искажении данных, вносимых в базы данных.

Причин, порождающих такие проблемы, множество, и в ограниченных рамках настоящей статьи перечислить их все невозможно, однако можно выделить основные проблемы, порождающие возможность несанкционированного доступа, хищения и искажения информации.

Первопричиной, по которой становится возможным несанкционированный доступ к базам данных и хищение из них информации, служит отсутствие соответствующих систем контроля за такими базами данных (такие системы контроля еще называют системы обнаружения вторжений). Действительно, если действия пользователя никто не анализирует и не контролирует, то его несанкционированные действия не будут вовремя замечены. Точно также при таком подходе нельзя своевременно выявить сбор информации из баз данных в целях неправомерного использования (распространения) со стороны уволенных или освобожденных от занимаемых должностей сотрудников органов внутренних дел. На практике территориальных органов МВД России выявлялись случаи, когда уволенные работники в течение года после увольнения имели действующие учетные записи от личного кабинета в базах данных. Обусловлено это тем, что практически все базы данных, с которыми работают в системе МВД России, в настоящий момент построены только по принципу контроля доступа через системы контроля доступом с расширенными правами. Традиционно системы контроля доступом контроля направлены именно на контроль за счет того определения, какие пользователи имеют право читать, изменять, добавлять и/или удалять информацию, но не на то,

чтобы объективно отслеживать, для каких целей используется информация, действующий ли сотрудник работает с информацией и правильно ли вносится информация в базы данных.

Для минимизации проблем, связанных с контролем доступа, необходимо внедрение эффективных систем обнаружения вторжений. Такие системы не добавляют никакой дополнительной безопасности, но вместе с тем предоставляют функционал для определения того, подвергается ли база данных угрозам. Систему обнаружения вторжений можно настроить для наблюдения за определенными типами действий пользователя, регистрации различных типов трафика в локальной сети для последующего анализа, контроля за ошибками при внесении информации и пр.

Заключение

Подводя итог, необходимо отметить, что в системе МВД России при работе с базами данных существует две группы проблем обеспечения информационной безопасности. Первая группа проблем — это проблемы надлежащей организации обеспечения безопасности. Такие проблемы первичны, и их наличие порождает вторичные проблемы – проблемы обеспечения информационной безопасности, связанные непосредственно с работой в базах данных: несанкционированный доступ к информации, ее хищение, а также искажение данных, вносимых в базы данных. Решить такие проблемы возможно за счет проведения комплекса мероприятий, направленных на обеспечение информационной безопасности, начиная с правильно организованного обучения информационной безопасности и заканчивая внедрением новых технологий в системы контроля. Обусловлено это тем, что необходимость обеспечения безопасности баз данных МВД России должна сбалансировать потребность в безопасности с потребностью пользователей в эффективном доступе и использовании этих баз данных, поскольку если меры безопасности баз данных недостаточно эффективны и неконтролируемы, то пользователи найдут способы обойти защиту и подвергнуть базы данным различным угрозам.

Библиография

1. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Российская газета. 06.12.2016.
2. Приказ МВД России от 18 января 2019 г. № 20 «Об объявлении решения коллегии МВД России от 5 декабря 2018 года № 2 км» // СПС «СТРАС ЮРИСТ».
3. Приказ МВД России от 14.03.2012 №169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» (ред. 26.10.2016) // СПС «СТРАС ЮРИСТ».
4. Приказ МВД России от 23.11.2016 №755 «Вопросы эксплуатации центра разработки, поддержки, внедрения и администрирования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России» (ред. 11.02.2020) // СПС «СТРАС ЮРИСТ».
5. Артамонова Я.С. К вопросу о понятии «Информационная безопасность» // Социально-гуманитарные знания. 2008. №1. С.319-321.
6. Бирюков А.А. Информационная безопасность: защита и нападение [Текст]: учеб. пособие/ А.А. Бирюков, Москва: ДМК Пресс. 2018. - 474с.
7. Кемпф В.А. Особенности субъективных угроз информационной безопасности информационных систем в деятельности органов внутренних дел Российской Федерации // Полицейская деятельность. 2019. №5. С.47-52.
8. Кубасов И.А., Стрельников Ф.И. Обеспечение безопасности функционирования инфокоммуникационных систем, используемых в следственной и судебно-экспертной деятельности // Академическая мысль. 2020. №3 (12). С.97-101.
9. Махмудова Н.Р., Мухамадиев С.И. Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения // Вопросы науки и образования. 2019. №16 (63). С.34-39.

10. Плахина Е.А. Компьютерные угрозы информационной безопасности // Наука и образование сегодня. 2019. №9 (44). С.35-36.
11. Ребрий А.Ю. Методы обеспечения информационной безопасности // Международный журнал прикладных наук и технологий «Integral». 2020. №3. С.369-379.
12. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 2 – 5.

Problems of ensuring information security in the system of the Ministry of Internal Affairs of Russia when working with databases

Aleksandr F. Efremov

Student
Management Academy of the Interior Ministry of Russia,
125171, 8, Zoi i Aleksandra Kosmodem'yanskikh str., Moscow, Russian Federation;
e-mail: postvim@mail.ru

Abstract

Today, global digitalization covers the whole world, affecting not only the life of society, but also the functioning of state authorities, and the Ministry of Internal Affairs of Russia, is no exception. So, for the last few years, the Ministry of internal Affairs of Russia has included in their core processes and management system, cloud technology, big data, the Internet, artificial intelligence, which in turn helped to organize and consolidate large amounts of information contained in analog disparate databases into a single information database. Such digital information databases have greatly increased the efficiency of the Ministry of Internal Affairs of Russia in its main area of activity –ensuring public safety and combating crime.

Nevertheless, when introducing digital technologies into the activities of the Ministry of Internal Affairs of Russia, there were problems related to ensuring information security. Analysis of the activities of the Ministry of Internal Affairs of Russia in terms of working with databases, led to the conclusion that in the Ministry of Internal Affairs of Russia for working with databases, there are two groups of problems of ensuring information security – the first group of problems is the problem of proper organization of security. Such problems are primary, and their presence gives rise to secondary problems – problems of ensuring information security directly related to working in databases: unauthorized access to information, its theft, as well as distortion of data entered into databases. It is possible to solve such problems by carrying out a set of measures aimed at ensuring information security, starting with properly organized information security training and ending with the introduction of new technologies in control systems.

For citation

Efremov A.F. (2020) Problemy obespecheniya informatsionnoi bezopasnosti v sisteme MVD Rossii pri rabote s bazami dannykh [Problems of ensuring information security in the system of the Ministry of Internal Affairs of Russia when working with databases]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 10 (11A), pp. 229-235. DOI: 10.34670/AR.2020.76.82.048

Keywords

Databases of the Ministry of Internal Affairs of Russia, information security, unauthorized access to information, information theft, information access control systems, data distortion

References

1. Ukaz Prezidenta RF ot 05.12.2016 №646 «Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii» // Rossiiskaya gazeta. 06.12.2016.
2. Prikaz MVD Rossii ot 18 yanvarya 2019 g. № 20 «Ob ob"yavlenii resheniya kollegii MVD Rossii ot 5 dekabrya 2018 goda № 2 km» // SPS «STRAS YuRIST».
3. Prikaz MVD Rossii ot 14.03.2012 №169 «Ob utverzhdenii Kontseptsii obespecheniya informatsionnoi bezopasnosti organov vnutrennikh del Rossiiskoi Federatsii do 2020 goda» (red. 26.10.2016) // SPS «STRAS YuRIST».
4. Prikaz MVD Rossii ot 23.11.2016 №755 «Voprosy ekspluatatsii tsentra razrabotki, podderzhki, vnedreniya i administrirovaniya servisov edinoi sistemy informatsionno-analiticheskogo obespecheniya deyatel'nosti MVD Rossii» (red. 11.02.2020) // SPS «STRAS YuRIST».
5. Artamonova Ya.S. K voprosu o ponyatii «Informatsionnaya bezopasnost'» // Sotsial'no-gumanitarnye znaniya. 2008. №1. S.319-321.
6. Biryukov A.A. Informatsionnaya bezopasnost': zashchita i napadenie [Tekst]: ucheb. posobie/ A.A. Biryukov, Moskva: DMK Press. 2018. - 474s.
7. Kempf V.A. Osobennosti sub"ektivnykh ugroz informatsionnoi bezopasnosti informatsionnykh sistem v deyatel'nosti organov vnutrennikh del Rossiiskoi Federatsii // Politseiskaya deyatel'nost'. 2019. №5. S.47-52.
8. Kubasov I.A., Strel'nikov F.I. Obespechenie bezopasnosti funktsionirovaniya infokommunikatsionnykh sistem, ispol'zuemykh v sledstvennoi i sudebno-ekspertnoi deyatel'nosti // Akademicheskaya mysl'. 2020. №3 (12). S.97-101.
9. Makhmudova N.R., Mukhamadiev S.I. Informatsionnaya bezopasnost' v sfere svyazi i informatizatsii. Problemy i puti ikh resheniya // Voprosy nauki i obrazovaniya. 2019. №16 (63). S.34-39.
10. Plakhina E.A. Komp'yuternye ugrozy informatsionnoi bezopasnosti // Nauka i obrazovanie segodnya. 2019. №9 (44). S.35-36.
11. Rebrii A.Yu. Metody obespecheniya informatsionnoi bezopasnosti // Mezhdunarodnyi zhurnal prikladnykh nauk i tekhnologii «Integral». 2020. №3. S.369-379.
12. Sukharenko A.N. Zakonodatel'noe obespechenie informatsionnoi bezopasnosti v Rossii // Rossiiskaya yustitsiya. 2018. № 2. S. 2 – 5.