РАЗВИТИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

DEVELOPMENT OF THE INFORMATION SECURITY SYSTEM OF INTERNAL AFFAIRS

УДК 004.056

Завгородний Евгений Николаевич, заместитель начальника центра информационных технологий, связи и защиты информации, Управление Министерства внутренних дел Российской Федерации по Камчатскому краю, Россия, г. Петропавловск-Камчатский

Zavgorodnii Evgenii Nikolaevich , ze2609@gmail.com

Аннотация

В статье приведен анализ состояния информационного обеспечения органов внутренних дел, перечислены основные направления системы обеспечения информационной безопасности, рассмотрены ее правовой, научный, организационно-технический, материально-технический и кадровый аспекты, доведены проблемные вопросы функционирования и развития системы, представлены предложения по их решению, сделан вывод о постоянном процессе функционирования, взаимосвязанности и неотделимости компонентов системы обеспечения информационной безопасности

Annotation

The article provides an analysis of the state of information support of the internal affairs agencies, lists the main directions of the information security system, considers its legal, scientific, organizational and technical, material and technical and personnel aspects, brings up problematic issues of the functioning and development of the system,

presents proposals for their solution, the conclusion was made about the constant process of functioning, interconnectedness and inseparability of the components of the information security system

Ключевые слова: информационная безопасность, органы внутренних дел, информационные системы, несанкционированный доступ, материально-техническое обеспечение, аудит безопасности.

Keywords: information security, internal affairs agencies, information systems, unauthorized access, material and technical support, security audit

Федеральный закон Российской Федерации от 07.02.2011 № 3-ФЗ «О полиции» провозгласил использование достижений науки и техники, современных технологий и информационных систем основным принципом деятельности полиции, законодательно закрепив инновационные процессы в правоохранительной сфере, и стимулировал внедрение инновационных продуктов мира цифровых технологий в деятельность органов внутренних дел (ОВД) [5, с. 1].

Современные условия деятельности ОВД неразрывно связаны с использованием информационно-телекоммуникационных технологий. В настоящее время происходит активное создание новых и модернизация ныне эксплуатируемых информационных ресурсов, централизация и подведение под единый формат представления и формирования разрозненных банков данных, которые позволяют сотрудникам ОВД различных направлений деятельности своевременно получать актуальные сведения, необходимые для выполнения своих функциональных обязанностей. Банки данных используются для сбора и обработки статистической, учетно-регистрационной информации, для организации оперативно-следственных мероприятий, проведения криминалистических исследований, управления деятельностью службами и подразделениями ОВД.

С учетом функций и полномочий, которыми наделяются правоохранительные органы, основные банки данных сконцентрированы в МВД России на федеральном и региональном уровнях.

В настоящее время существует необходимость в быстром и надежном получении сведений, используемых в правоохранительной деятельности по различным физическим и логическим каналам передачи данных.

Вместе с тем, активное развитие технологий и их постоянное внедрение в деятельность ОВД неразрывно связано с необходимостью реализации многоуровневой системы обеспечения информационной безопасности (ИБ), необходимостью ее своевременного развития и модернизации.

МВД России уделяется значительное внимание обеспечению ИБ. В рамках осуществления данной деятельности, производится комплекс мероприятий по защите информации, содержащей сведения, составляющие государственную тайну, и сведения конфиденциального характера.

В соответствии с Концепцией обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (Концепция), защищенность информации достигается комплексом мер, реализуемых функционированием системы обеспечения ИБ. В свою очередь, система обеспечения ИБ является совокупностью правовых, организационных и технических мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам ИБ с целью предотвращения либо существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней [2, с. 6].

Основными направлениями обеспечения ИБ в ОВД являются:

- совершенствование нормативной правовой базы по ИБ;
- выработка основных направлений единой научно-технической политики в области обеспечения ИБ;
- реализация способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз ИБ;

- организация технической, криптографической защиты информации, а также защиты информации от несанкционированного доступа к информационным ресурсам ОВД;
- обеспечение ИБ при межведомственном информационном взаимодействии с федеральными органами государственной власти;
- проведение технического аудита состояния защищенности информационных систем ОВД;
- совершенствование профессиональной подготовки сотрудников органов внутренних дел в области защиты информации на базе образовательных учреждений системы МВД России;
- совершенствование материально-технической базы ОВД, в том числе ведомственных образовательных учреждений.

С точки зрения взглядов на действующую систему ИБ ОВД, можно выделить следующие аспекты, позволяющие более конкретно изучить составляющие системы: правовой, научный, организационно-технический, материально-технический и кадровый.

Правовой аспект системы обеспечения ИБ включает в себя разработку проектов законодательных, подзаконных и межведомственных нормативных правовых актов в области защиты информации, в том числе их соответствие требованиям регуляторов в области обеспечения защиты информации Российской Федерации. Актуальным вопросом является включение мероприятий по защите информации в федеральные и ведомственные целевые программы на стадии их планирования и утверждения, а также реализация мероприятий в системе государственных заказов на продукцию, товары и услуги в области защиты информации.

Имеется необходимость в формировании алгоритма постановки в качестве используемой на вооружении актуальной и соответствующей действующим требованиям безопасности информации продукции, используемой в целях защиты информации в МВД России, а также в формировании порядка планирования и своевременной модернизации эксплуатируемой техники защиты

информации, с учетом сроков действия сертификатов соответствия на используемое оборудование и сроков оказания технической поддержки производителем продукции .

Научный аспект системы обеспечения ИБ предусматривает формирование научно-технической базы на основе планирования, проведения и внедрения результатов научно-исследовательских и опытно-конструкторских работ, учета передового опыта, реализации единой научно-технической политики по созданию, совершенствованию и развитию системы безопасности, разработки соответствующих единых централизованных технических решений по ее созданию и эксплуатации.

Отсутствие унифицированного технического решения по обеспечению безопасности информации в используемых региональных информационных системах негативно влияет на эффективность применения соответствующих организационно-технических и экономических мер в части финансирования и внедрения средств защиты информации. В условиях ограничения финансирования деятельность по информационному обеспечению ОВД возможна только с применением передового опыта в области информационных технологий и выработанных единых решений.

Организационно-технический аспект системы обеспечения ИБ включает в себя совершенствование деятельности подразделений ОВД, в функции которых входит обеспечение технической и криптографической защиты информации, а также эксплуатация информационных ресурсов. Данные мероприятия предусматривают реализацию полного этапа жизненного цикла информационной системы, начиная от ее проектирования и организации разрешительной системы доступа к информационным ресурсам ОВД, распределения ответственности при обработке информации, а также определения процедур по выявлению информационно-технических воздействий на информационную сферу ОВД, до проведения мероприятий по ее аттестации, сопровождения при функционировании и вывода из эксплуатации.

Одним из условий функционирования системы обеспечения ИБ в информационных системах в части обеспечения целостности, доступности информации является гарантированная стойкость конфиденциальных каналов связи, обеспечение бесперебойного функционирования и резервирования информационно-телекоммуникационных систем ОВД. Немаловажным условием реализации мер защиты является размещение коммуникационного, каналообразующего оборудования, а также серверов хранения данных и оконечных абонентских мест доступа к информационным ресурсам в контролируемой зоне объектов ОВД.

В целях предупреждения возникновения угроз безопасности информации в информационных ресурсах ОВД целесообразно внедрение централизованной системы мониторинга, включающей в себя систему прогнозирования возможности возникновения угроз, реагирования на инциденты безопасности, а также ликвидации и устранения последствий инцидентов безопасности информации.

Функционирование системы обеспечения ИБ предусматривает периодическое проведение комплексного контроля выполнения требований нормативных правовых, нормативных технических и методических документов по вопросам обеспечения ИБ и соответствующего технического (инструментального) контроля эффективности реализованных мер защиты, а также совершенствования взаимодействия головных и подчиненных подразделений по координации и методическому сопровождению их деятельности.

Материально-технический аспект системы обеспечения ИБ включает в себя оснащение программными, программно-аппаратными средствами защиты информации (включая криптографические), необходимыми для организации технической защиты информации, их закупку и поставку в ОВД в объемах, предусмотренных нормами положенности. С учетом темпов развития рынков информационных технологий, возрастающих задач по информатизации ОВД, проблемным вопросом остается классификация и типизация при определении

потребности в средствах защиты информации. В связи с этим, а также с неблагоприятной политической и экономической ситуациями, необходимостью функционирования деятельности ОВД в условиях распространения новой коронавирусной инфекции, имеется необходимость оптимизации работ, связанных с закупкой и поставкой средств защиты информации через систему государственных заказов. Проблему формирования государственного заказа по линии защиты информации возможно решить путем утверждения типов (классов, норм) используемого оборудования, средств технической (криптографической) защиты информации, в зависимости от топологии используемых сетей, особенностей функционирования информационных систем в регионах, а также конкретных задач, выполняемых подразделениями по защите информации ОВД.

Возможность возникновения угроз безопасности при использовании зарубежных информационных систем, программного обеспечения и аппаратных средств вынуждают форсировать мероприятия по переходу на отечественные программно-аппаратные платформы. Существует проблема совместного использования имеющихся на отечественном рынке средств защиты информации и отечественных операционных систем, а также возможности их интеграции в состав информационных ресурсов ОВД. В этих условиях следует стремиться к поддержанию максимально возможного уровня обеспечения ИБ, достижения сбалансированности и устойчивости системы. Необходимо поэтапное планирование мероприятий по достижению определенного уровня безопасности с возможностью корректировки системы государственного заказа, а также по переходу на использование отечественного программного обеспечения, с учетом проводимого аудита ИБ.

Кадровый аспект системы обеспечения ИБ предусматривает организацию подготовки и повышения квалификации сотрудников ОВД по направлениям деятельности в области обеспечения ИБ на базе ведомственных образовательных учреждений, а также повышение «компьютерной грамотности» и «культуры ИБ» у сотрудников ОВД при выполнении ими своих служебных обязанностей.

Ключевым моментом развития кадрового потенциала является определение приоритетных направлений профессиональной подготовки (переподготовки), исходя из актуальных угроз безопасности информационным ресурсам ОВД.

В целях реализации единого подхода к проведению мероприятий по защите информации необходимо приведение организационно-штатной структуры подразделений по защите информации на федеральном, региональном и районном уровнях в соответствии с предъявляемыми нормативной базой требованиями.

Также, одной из ключевых задач является формирование цифровой компетентности современного образования сотрудников ОВД, каждый из которых в повседневной деятельности использует информационные ресурсы ОВД, независимо от своих функциональных обязанностей [5, с. 2].

Проведение «массового» повышения квалификации сотрудников ОВД в части, касающейся обработки информации в информационных системах, а также по обеспечению безопасности информации на уровне пользователя, существенно перераспределит нагрузку на специализированные подразделения по защите информации в сторону концентрации деятельности по проведению организационно-технических мероприятий по обеспечению безопасности информации.

Таким образом, исследуя систему обеспечения ИБ в ОВД, можно сделать вывод, что мероприятия по поддержанию ее работоспособности и являются взаимозависимыми, процесс функционирования системы является цикличным и непрерывным, каждый из рассмотренных аспектов не имеет приоритета над остальными, способность системы выполнять свою функцию реализовывается одновременным развитием по всем ее направлениям.

Литература

1. Лебедев В.Н. и др. под ред. Кирина В.И. Защита информации: учебник в 2-х частях // Академия управления МВД России. 2013. – 260 с.

2. Приказ МВД России от 14 марта 2012 г. N169 «Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 г.». Доступ из справочно-правовой системы «Страс-ЮРИСТ».
3. Указ Президента России от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ из справочно-правовой системы «Консультант-плюс».
4. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России, 2012. - 98 с.
5. Шпагина Е. М. Формирование цифровой компетентности у сотрудников полиции. [Электронный ресурс]. URL: http://petrovka-38.com/arkhiv/item/formirovanietsifrovoj-kompetentnosti-u-sotrudnikov-politsii (дата обращения: 05.06.2021).
6. Попов А. Ю., Рак И. П. Информационные технологии в деятельности правоохранительных органов. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-deyatelnosti-pravoohranitelnyh-organov (дата обращения: 05.06.2021).

Literature

1. Lebedev V.N. and others, ed. Kirina V.I. Information security: a textbook in 2 parts // Academy of Management of the Ministry of Internal Affairs of Russia. 2013 .- 260 p.
2. Order of the Ministry of Internal Affairs of Russia of March 14, 2012 N169 "Concept of ensuring information security of the internal affairs bodies of the Russian Federation until 2020". Access from the reference and legal system "Strass-JURIST".
3. Decree of the President of Russia of 05.12.2016 N 646 "On the approval of the Doctrine of information security of the Russian Federation." Access from the reference and legal system "Consultant-plus".

4. Beloglazov E.G. and other Fundamentals of information security of internal affairs agencies: Textbook. - M .: MosU of the Ministry of Internal Affairs of Russia, 2012 .- 98 p.
5. Shpagina EM Formation of digital competence among police officers. [Electronic resource]. URL: http://petrovka-38.com/arkhiv/item/formirovanietsifrovoj-kompetentnosti-u-sotrudnikov-politsii (date of access: 05.06.2021).
6. Popov A. Yu., Cancer IP Information technologies in the activities of law enforcement agencies. [Electronic resource]. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-deyatelnosti-pravoohranitelnyh-organov (date of access: 05.06.2021).