ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

УДК 12.00.12

Особенности совершенствования информационной безопасности в органах внутренних дел Российской Федерации

Жуков Азамат Заурбекович, кандидат технических наук,
старший преподаватель кафедры деятельности ОВД в особых условиях
Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России (г. Нальчик)

Аннотация. *В данной статье представлен обзор проблем обеспечения информационной безопасности в системе органов внутренних дел. Рассмотрена программа, ключевыми целями которой является совершенствование системы информационной безопасности в органах внутренних дел. Данная проблема является актуальной, так как именно органы внутренних дел являются одним из основных инструментов обеспечения эффективной системы защиты информации.*

Ключевые слова: *информационная безопасность, органы внутренних дел, информатизация, информационные процессы, информационные данные.*

Информационные процессы охватывают все больше сфер жизнедеятельности общества. Информатизация современного общества является глобальным процессом, для которого характерны высокие темпы развития. В 21 веке именно информация является ключевым средством, которое может нанести вред целостности и безопасности государства. Так многие информационные процессы подвергаются воздействию с целью причинения вреда стабильному развитию общества. Это негативным образом сказывается на степени эффективности защиты общества.

Выше сказанное свидетельствует о необходимости формирования эффективной и целостной системы обеспечения информационной безопасности на всех уровнях: безопасность физических и юридических лиц, безопасность государства в целом. [1]

В Российской Федерации в условиях становления рыночных отношений, активной глобализации экономической сферы, роста количества транснациональных преступлений, угрозы информационной безопасности имеют особую актуальность. Следует также отметить, что угрозу информационной безопасности в определенной степени наносят политические конфликты с западными странами и международный терроризм.

Ошибочно полагать, что защита информации сводится исключительно к защите цифровой информации, поскольку обеспечение защиты информации носит многоаспектный характер. Так, можно выделить четыре аспекта:

– нормативно-правовой аспект, который включает в себя законы различного уровня, нормативные акты, стандарты и т.п.;

– административный аспект, под которым подразумевается деятельность руководства;

– процедурный аспект, который включает систему мер безопасности, направленных на контроль за соблюдением сотрудниками мер по обеспечению информационной безопасности;

– программно-технический аспект, который включает технические и программные мероприятия, направленные на обеспечение информационной безопасности.

В целях повышения эффективности обеспечения информационной безопасности в России предприняты организационные и правовые меры. В основном это касается разработки правовых и организационно-административных механизмов, направленных на защиту информации конфиденциального характера от криминальных структур.

Разработка эффективной нормативно-правовой системы, направленной на противодействие и нейтрализацию угроз физическим и юридическим лицам, обществу и государству является одним из ключевых векторов повышения эффективности безопасности информации.

Органы внутренних дел выступают в качестве одного из основных звеньев в механизме обеспечения информационной безопасности. Обеспечение национальной безопасности и информационной безопасности в частности является и одной из важнейших функций системы органов внутренних дел.

Органы внутренних дел МВД России осуществляют информационную борьбу с транснациональными и национальными сообщества, совершающими преступления. Информационная борьба органов внутренних дел связана с применением специальных информационно-вычислительных средств, радиосредств, средств технической разведки и других информационных ресурсов.

В Российской Федерации действует ряд документов, разработанных в целях обеспечения информационной безопасности. В качестве основного документа следует отметить Доктрину информационной безопасности Российской Федерации. В данном документе обозначены национальные интересы в информационной сфере, защита которых входит в сферу деятельности органов внутренних дел.[2]

В органах внутренних дел программы, направленные на совершенствование информационной защиты следует рассматривать с трех позиций:

– защита информационных данных от воздействия информационными инструментами, применя-

[1] Журавленко Н.И., Кадулин В.Е., Борзунов К.К. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2012.

[2] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

емыми в качестве механизма осуществления силовой политической борьбы;

– роста количества экономических преступлений в коммерческой и государственной сферах;

– защита информации служебного характера, которая составляет государственную тайну в деятельности органов внутренних дел.

В рамках первого аспекта необходимо обеспечить систематический контроль средств и систем информационной техники, средств связи, а особенно компьютерной техники зарубежного производства, которые поступаю на вооружение в органы внутренних дел. Кроме того, необходимо обеспечить также, контроль за включением различных комплектующих элементов программных и технических закладных устройств, управляемых внешними командами и приводящих к уничтожению, отказам или возможности несанкционированного снятия информации, циркулирующей в технологическом контуре управления органами внутренних дел.

Рост количества компьютерных преступлений в сфере экономики, деятельности государственных органов и коммерческих структур обусловил разработку программы совершенствования защиты информации в Министерстве внутренних дел Российской Федерации.

Проведенные социологические исследования свидетельствуют, что с начала 21 века преступления, совершаемые в сфере экономики, будут ориентированы именно на совершение несанкционированных действий преступного характера в информационных системах экономической и банковской сфер.

Высокая латентность характерна для преступлений, совершаемых в сфере цифровой экономики. В Российской Федерации часто фиксируются именно преступления данного характера. Для решения данной проблемы необходимо вести систематическую работу по подготовке криптоаналитиков для органов внутренних дел.

В качестве одного из таких инструментов можно рекомендовать формирование центров криптоаналитической обработки информации в регионах, которые будут оснащены всем необходимым оборудованием и специалистами высокого профессионального уровня. Данная подготовка может быть реализована на базе Института криптографии, связи и информатизации Федеральной службы безопасности Российской Федерации.

В рамках третьего направления необходимо выстроить надежную систему защиты информации в структурных подразделениях и службах органов внутренних дел. [3]

Методы, направленные на защиту информации от несанкционированного снятия, уничтожения и модификации можно распределить по двум категориям:

— защита аналоговых каналов от несанкционированного воздействия;

— защита цифровых каналов от несанкционированного воздействия.

Данная классификация может быть детализирована по типам объектов защиты:

— стационарные объекты защиты информации;

— временные объекты защиты информации МВД России.

В качестве основной цели Программы выступает совершенствование системы обеспечения безопасности информации, которая циркулирует в каналах информации органов внутренних дел. Сопутствующими целями программы являются разработка, адаптация средств и методов выявления различного рода радиозакладных устройств, которые устанавливаются в служебных помещениях органов внутренних дел.

Эффективность обеспечения информационной безопасности зависит от ряда внешних и внутренних факторов: политических, экономических и организационно - технических.

К политическим факторам относятся:

— резкое изменение геополитической ситуации вследствие кардинальных перемен в мире;

— информационная экспансия развитых стран, которые осуществляют мониторинг глобальных проблем;

— формирование новой формы российской государственности, выстроенной на принципах демократии, информационной открытости;

— стремление Российской Федерации к построению более тесной формы сотрудничества с западными и европейскими государствами в процессе реализации реформ, направленных на максимальную открытость сторон;

— низкий уровень информационной и правовой культуры в обществе.

В качестве наиболее существенных экономических факторов отметим следующие:

— низкий уровень производимых отечественными предприятиями промышленности технических средств защиты информации и информатизации;

— создание транснациональных организаций по развитию информационной инфраструктуры России

Тяжело положение в области обеспечения эффективной системы информационной безопасности требует решения обозначенных выше проблем.

Необходимо развитие научных и практических основ информационной безопасности, которые будут отвечать современным мировым тенденциям, а также условиям социально-экономического и политического развития Российской Федерации.

Одним из инструментов построения современной системы информационной безопасности в органах внутренних дел является формирование нормативно-правового фундамента обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса и регламента информационного обмена для МВД России.

В качестве технической составляющей следует разработать современные методы и технические средства, которые позволят комплексно решить актуальные задачи защиты информации.

В структуре МВД Российской Федерации стоит разработать критерии и методы оценки эффективности систем и средств информационной безопасности,

[3] Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России, 2012.

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

а также требования к их сертификации

Одним из важных факторов, как мы отмечали ранее, является уровень информационной грамотности персонала. Комплексное исследование деятельности персонала, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.[4]

Проведенный выше анализ современного состояния системы обеспечения информационной безопасности в органах внутренних дел позволяет сформировать ряд выводов:

1. Органы внутренних дел являются ключевым звеном в системе обеспечения информационной безопасности. Также органы внутренних дел выступает в качестве основных исполнителей положений, которые обозначены в Доктрине информационной безопасности и ряде иных нормативно-правовых актов в сфере регулирования информационной безопасности.

2. Для проблемы информационной безопасности характерен комплексный характер и зашита информации должна выстраиваться на всех уровнях: техническом, административном, процедурном, законодательном. В качестве угрозы информационной безопасности стоит рассматривать не только иностранные государства и террористические организации, но и также организованная преступность.

3. Основными направлениями реализации органами внутренних дел национальных интересов в сфере информационной безопасности, являются:

— обеспечение реализации права граждан на информацию;

— обеспечение функционирования информационной инфраструктуры;

— противодействие распространению опасной и вредной информации.

4. В рамках реализации права граждан на получение информации о деятельности органов внутренних дел и органов исполнительной власти, в данный момент имеются множественные нарушения, которые отчасти обусловлены низкой правовой активностью граждан, и массовостью данного явления.

Таким образом, совершенствование системы информационной безопасности органов внутренних дел позволит значительно повысить уровень информационной и национальной безопасности государства. Разработанная Доктрина по информационной безопасности позволяет системно решить обозначенные проблемы и значительно повысить уровень информационной безопасности в правоохранительной системе Российской Федерациии и государстве в целом.

Литература:

1.Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

2.Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. - М.: МосУ МВД России, 2012. - 98 с.

3.Журавленко Н.И., Кадулин В.Е., Борзунов К.К. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России. 2012. - 190 с.

4.Панов, А. Ю. Особенности эффективной организации оперативно-розыскной деятельности по выявлению налоговых преступлений / А. Ю. Панов // Проблемы экономики и юридической практики. 2017. № 4. С. 86–89.

5.Попова Д. И. Совершенствование информационного обеспечения оперативно-розыскной деятельности органов внутренних дел (по материалам УМВД России по г. Севастополю) // Молодой ученый. — 2018. — №49. — С. 155-157. — URL https://moluch.ru/archive/235/54517/ (дата обращения: 11.07.2019).