Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра
экономики, финансового права и информационных технологий в деятельности ОВД

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему:
«Обеспечение информационной безопасности в органах внутренних дел Российской Федерации»

Выполнил: Яруллин Рузель Маратович
(фамилия, имя, отчество)
ПОНБ, 2013, 131 уч. Группа
(специальность, год набора, № группы)

Руководитель:
к.п.н., доцент, подполковник полиции
(ученая степень, ученое звание, должность
Турутина Елена Эдуардовна
(фамилия, имя, отчество)

Рецензент:
Начальник Отдела дознания ОМВД России по Альметьевскому району подполковник полиции
(должность, специальное звание)
Смоленкова Гульназ Мансуровна
(фамилия, имя, отчество)

К защите допущена 14.05.18.
(допущена, дата)
Начальник кафедры

Оценка _____

Дата защиты: "___" _____2018 г.

Казань 2018

Содержание

ВВЕДЕНИЕ

Актуальность темы исследования. Информационная безопасность – это достаточно новая область научной и практической деятельности, связанная с государственными, общественными и личными интересами граждан, обусловленная тем, что в результате развития современного общества наметилась устойчивая тенденция перехода его к качественно новому состоянию, именуемому информационным обществом. При этом одной из важнейших проблем стала проблема обеспечения именно безопасности информации.

Сложность решения проблемы обеспечения информационной безопасности заключается в постоянном появлении все новых угроз в информационной сфере (информационные войны, информационный терроризм, экономические преступления в финансовых, банковских компьютерных системах с использованием современных информационных технологий и т.д.).

В последнее время проблема информационной безопасности рассматривается шире. Оказалось, что современные технические, технологические и организационные системы, а также люди, коллективы людей и общество в целом сильно подвержены внешним информационным воздействиям, причем последствия негативного воздействия могут носить очень тяжелый характер.

Особую остроту эта проблема находит в деятельности органов, имеющих непосредственное отношение к задачам обеспечения защиты государства от угроз внешнего и внутреннего характера. Важное место в этой проблеме занимают органы внутренних дел, деятельность которых, как части единой государственной структуры – МВД России, неразрывно связана с интересами общества и государства в правоохранительной сфере.

В нынешних условиях проблема защиты информации в деятельности

органов внутренних дел приобрела особую актуальность, т.к. систематизированная в результате их деятельности информация представляет огромный интерес как для отдельных криминальных элементов и группировок, так и для организаций антиконституционной направленности, партий, общественно-политических движений и средств массовой информации, стремящихся использовать для своих целей оперативно-служебную информацию органов внутренних дел. В процессе осуществления служебной деятельности сотрудники органов внутренних дел получают информацию о режиме и характере работы предприятий, расположенных на обслуживаемой территории, о характере и особенностях работы режимных предприятий, а также другие виды информации, не предназначенной для ознакомления с ней посторонних лиц. Нередко эта информация составляет государственную тайну.

В органах внутренних дел уделяется особое внимание вопросам сохранения секретных сведений, воспитанию у сотрудников высокой бдительности. Однако некоторыми из них часто недооценивается опасность утечки информации ограниченного доступа. Они проявляют граничащую с преступной халатностью беспечность при обращении с секретными документами, в том числе и в электронном виде, что нередко приводит к разглашению сведений, составляющих государственную тайну, и даже к утрате секретных документов и файлов. Низкие профессиональные качества отдельных сотрудников нередко ведут к нарушению конфиденциальности доверенной им информации. Перечисленные недостатки в деятельности органов управления зачастую приводят к утечке секретных сведений, и неминуемым следствием таких процессов является возрастание угрозы безопасности России.

Законодательные и исполнительные органы власти России придают большое значение мерам по защите информации, в государственных правовых и ведомственных нормативных актах строго регламентированы меры по обеспечению режима секретности и защите сведений, составляющих

государственную, служебную, профессиональную, коммерческую, личную тайну.

Актуальность избранной темы определяется как возрастанием требований к органам внутренних дел, связанных с совершенствованием их профессиональной деятельности на современном этапе развития правоохранительной системы государства, так и возрастанием роли информационной безопасности в деятельности органов внутренних дел в целом.

Степень разработанности темы исследования. Проведенный автором анализ результатов исследований ученых позволяет констатировать, что проблемы правового регулирования информационных отношений, обеспечения информационной безопасности и ее компонентов являются актуальными для правовой науки и практики и требуют дальнейшего развития». Значительное количество публикаций посвящено частным проблемам и вопросам правового регулирования отношений в информационной сфере, сфере информационной безопасности, обеспечения безопасности информации, предполагающей ее защиту от хищения, утраты, несанкционированного доступа, копирования, модификации, блокирования и т.п., рассматриваемых в рамках формируемого правового института тайны. Большой вклад в развитие данного направления внесли отечественные ученые и специалисты: А. Б. Агапов, В. И. Булавин, Ю. М. Батурин, С. А. Волков, В. А. Герасименко, В. Ю. Гай-кович, И. Н. Глебов, Г. В. Грачев, С. Н. Гриняев, Г. В. Емельянов, В. А. Копылов, А. П. Курило, В. Н. Лопатин, А. А. Малюк, А. С. Прудников, С. В. Рыбак, А. А. Стрельцов, А. А. Фатьянов, А. П. Фисун, В. Д. Циганков, Д. С. Черешкин, А. А. Шиверский и др.

Объектом исследования является действующая и формирующаяся системы общественных отношений, сложившихся в информационной сфере и сфере информационной безопасности.

Предметом исследования являются международно-правовые акты, содержание Конституции Российской Федерации, нормы отечественного

законодательства, регулирующие отношения в области обеспечения информационной безопасности личности, общества и государства, а также содержание правовых норм, регулирующих деятельность органов внутренних дел по обеспечению информационной безопасности.

Цели выпускной квалификационной работы – изучить современное состояние обеспечения информационной безопасности в органах внутренних дел Российской Федерации.

Задачи выпускной квалификационной работы:

1. Изучить понятие и сущность информационной безопасности.

2. Рассмотреть нормативно-правовое регулирование информационной безопасности в Российской Федерации.

3. Раскрыть роль ОВД в обеспечении информационной безопасности РФ.

4. Раскрыть организационные основы информационной безопасности в органах внутренних дел.

Методологическую основу выпускной квалификационной работы составляют всеобщие философские методы и принципы материалистической диалектики; общенаучные методы сравнения, обобщения, индукции; частно-научные методы: системно-структурный, системно-деятельностный, формально-юридический, сравнительно- правовой и другие методы исследования.

Нормативную базу исследования составляют Конституция Российской Федерации, нормативные правовые акты Российской Федерации в том числе, международное законодательство, нормы различных отраслей права, ведомственные нормативные акты.

Структура выпускной квалификационной работы состоит из введения, двух глав, заключения, списка литературы.

ГЛАВА I. ПОНЯТИЕ И ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Понятие и сущность информационной безопасности

В современном мире проблемы информационной безопасности приобрели глобальные масштабы и превратились в фактор, влияющий на выживание человечества. Традиционные методы безопасности не выполняют своих функций и под влиянием новых информационных технологий трансформируются, что приводит к появлению новых форм информационной опасности. Вот почему Всемирная федерация ученых в августе 2000 года, первая угроза человечеству в XXI веке, создала угрозу информационной безопасности.

Таким образом, безопасное развитие любого современного общества, государства, человека в современном мире напрямую связано с их информационной безопасностью, поскольку информационная среда в наши дни является системообразующим фактором социального развития. Информационная безопасность характеризуется способностью государства, общества, социальной группы, индивида предоставлять с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные усилия для поддержания средств к существованию и жизнеспособности, противодействия информационным угрозам и угрозам, негативное воздействие информации на индивидуальное и общественное сознание и психика людей, а также на компьютерных сетях и других технических источниках информации, осуществлять информационно-психологическую конфессиональную конфронтацию.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности

Российской Федерации[1] термин «информационная безопасность» используется в широком смысле, а это означает состояние защиты национальных интересов в информационной сфере, определяемое сочетанием сбалансированных интересов личности, общества и государства.

Согласно Е.Н. Пасхину, теперь можно вполне обоснованно утверждать, что человеческая цивилизация - это в основном технологическое общество[2]. Но в то же время проблему безопасного технологического развития страны следует рассматривать как национальную проблему экономического выживания и будущего безопасного развития.

В рамках новой информационной стратегии социального развития безопасность и развитие (саморазвитие) были настолько взаимосвязаны, что обеспечить безопасность цивилизации в принципе невозможно без перехода к пути безопасного развития. И наоборот, устойчивое развитие, то есть сохранение человеческой культуры и биосферы, невозможно без обеспечения их совместной безопасности. Отличительной чертой новой модели безопасности в системе современного развития является то, что она должна развиваться, отходить от общего принципа классической безопасности «вызов-ответ».

Опережающая модель безопасности раскрывается в трудах А.Д. Урсула[3], Ю.Л. Кутахова[4], Р.А. Явчуновской[5] и других. Они раскрывают смысл опасностей, угрожающих стране, конкретному человеку, доказывают необходимость сосредоточиться на знаниях, традициях, идеалах, которые призваны обеспечить безопасность общества, природы и человека, их устойчивое сосуществование, механизмы их преодоления.

---

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” // Собрание законодательства Российской Федерации. – 2016. - №50. – Ст. 7074.

[2] Пасхин, Е.Н. Устойчивое развитие и информатизация образования / Е.Н. Пасхин, В.Г. Тупало, А.Д. Урсул. М.: Изд-во РАГС. 2007. – С. 122.

[3] Пасхин, Е.Н. Устойчивое развитие и информатизация образования / Е.Н. Пасхин, В.Г. Тупало, А.Д. Урсул. М.: Изд-во РАГС. 2007. – С. 122.

[4] Кутахов, Ю.Л. Человек. Полиэтнический мир. Безопасность / Ю.Л. Кута- хов , Р. А. Явчуновская. СПб., 1998. 404 с.

[5] Немыкина О. И. Теоретический анализ проблем информационной безопас- ности современного общества Теория и практика общественного развития. 2011. № 1. С. 43.

В общем, информационная безопасность общества и государства означает состояние отсутствия информационных угроз и угроз (отсутствие опасного информационного воздействия извне) и, если они существуют, состояние устойчивости основных сфер жизни, существование устойчивых связей между основными сферами общества (политика, экономика, общественное сознание и т.д.).

Анализ определений «информационной безопасности», предложенный учеными или закрепленный в нормативных документах, указывает на его определение как «состояние защиты национальных интересов в информационном поле».

Конкретизируя термин «информационная сфера», формулирует понятие Л. К. Терещенко: «информационная безопасность – состояние защищенности национальных интересов Российской Федерации в информационной сфере, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений»[6].

Некоторые авторы обосновывают это явление за счет наличия угрозы, то есть определяют информационную безопасность как состояние защиты национальных интересов в информационной сфере от внутренних и внешних угроз.

Один из подходов нашел отражение в работах технических ученых. Они сводят информационную безопасность главным образом к деятельности по защите свойств информационной и информационной инфраструктуры за счет технических и организационных мер, основанных на положениях государственных стандартов[7].

---

[6] Терещенко Л. К Модернизация информационных отношений и информационного законодательства: Монография. – М. : ИНФРА-М. – 2013. – С. 158.

[7] Холопова Е. Н., Бойцов А. С. Информационная безопасность пограничных органов на современном этапе: понятие, структура // Информационное право. – 2014. – № 5. – С. 6.

Необходимо различать определение информационной безопасности не через состояние защиты национальных интересов, а через способность и способность юридических лиц обеспечивать, защищать и развивать информационную сферу.

Различные научные подходы к понятию «информационная безопасность»: от широкого - «состояние защиты национальных интересов в информационной сфере от внутренних и внешних угроз» (в том числе огромное количество мероприятий, от конфронтации в информационных войнах до защиты личных данных отдельного гражданина) к узкой «деятельности по защите свойств информации» - и отсутствие ее консолидации в федеральных правилах затрудняет научно понять такие важные составляющие элементы информационной безопасности, как ее структура и система[8].

Очевидно, что необходимо различать понятия «информационная безопасность Российской Федерации», «безопасность информационной сферы», «защита информационной и информационной структуры».

В сегодняшнем мире существует несколько подходов к информационной безопасности, которые отличаются друг от друга. Приоритетным направлением первого подхода является обеспечение информационной открытости, а второе направление - дозирование информации, обеспечивающее контроль доступа к ней.

Ранее в нашей стране проблема правового обеспечения информационной безопасности не только не была выдвинута, но и фактически полностью игнорировалась. В настоящее время возрастает роль и значение информационной безопасности в рамках обеспечения национальной безопасности Российской Федерации по следующим основаниям.

Во-первых, одной из основных причин необходимости поддержания информационной безопасности на высоком уровне является развитие

[8] Холопова Е. Н., Бойцов А. С. Информационная безопасность пограничных органов на современном этапе: понятие, структура // Информационное право. – 2014. – № 5. – С. 6.

информатизации общества. Исследования показывают, что развитие экологической информационной среды оказывает значительное влияние на социальный прогресс и развитие каждого человека. Поэтому информационная среда нуждается в надежной защите, в том числе в правовой.

Во-вторых, в контексте глобализации роль информации растет. Его можно разумно считать объектом и продуктом труда, одним из основных активов страны, а также стратегическим национальным ресурсом.

В-третьих, в политической сфере приобретает все большее значение не столько власть, сколько информационные факторы. Например, возможности использовать интеллектуальный потенциал других стран, распространять и внедрять свои духовные, идеологические ценности, свою культуру, язык, возможности препятствовать духовному и культурному развитию других стран, трансформировать и даже подрывать их духовные и моральные основы[9].

Кроме того, нельзя не учитывать тот факт, что прямо пропорциональные отношения можно проследить между научно-техническим прогрессом и информационной безопасностью личности, общества и государства. По мере развития науки и техники возрастает роль и значение информационной безопасности.

Многие исследователи в определении понятия «информационная безопасность» определяют основной компонент - защиту отдельных, общественных, государственных и информационных ресурсов от воздействия на них информационных и психологических угроз[10].

Технические инновации виртуализации и глобализации не означают радикальных изменений в самом обществе. Главную роль играет трансформация не в материи, а в сознании - как индивидуальном, так и социальном[11].

---

[9] Козориз Н. Л. Информационная безопасность в системе противодействия опасности // Информационное право. – 2013. – № 1. – С. 30.

[10] Кутахов, Ю.Л. Человек. Полиэтнический мир. Безопасность / Ю.Л. Кута- хов , Р. А. Явчуновская. СПб., 1998. – С. 70.

[11] Зейналов, Г.Г. Глобализация как фактор современного развития / Г.Г.Зейналов, О.И. Немыкина // Учебный

Основные понятия в области защиты информации определяет ГОСТ Р 50922-2006. Рассмотрим базовые понятия из области информационной безопасности.

Информационная безопасность - действия, направленные на предотвращение утечки защищенной информации, а также несанкционированное и непреднамеренное воздействие на защищенную информацию.

Различают следующие виды защиты информации:

- юридические;
- технические;
- криптографический;
- физический.

Правовая защита информации - защита информации юридическими методами, в том числе разработка законодательных и нормативных правовых актов (актов), регулирующих отношения юридических лиц для защиты информации, применения этих документов (актов), а также надзора и мониторинга их реализации.

Техническая защита информации - это защита информации, которая заключается в предоставлении некриптографических методов защиты информации (данных), подлежащих (подлежащей) защите в соответствии с действующим законодательством, с использованием технического, программного и программного обеспечения.

Криптографическая защита информации - защита информации посредством криптографических преобразований.

Физическая защита информации - защита информации посредством использования организационных мер и набора средств, которые создают препятствия проникновению или доступу неавторизованных лиц к объекту защиты.

эксперимент в образовании. 2011. № 2. С. 4.

Меры по обеспечению информационной безопасности должны осуществляться не только в разных сферах - политике, экономике, обороне, но и на разных уровнях - государственной, региональной, организационной и личной. Поэтому задачи информационной безопасности на государственном уровне отличаются от задач, стоящих перед информационной безопасностью на уровне организации. Если в первом случае речь идет об обеспечении национальных интересов, то во вторых решаются частные задачи - формирование и поддержание имиджа организации, борьба с клеветой и дезинформацией от противников и т.д.[12]

В настоящее время могут быть выявлены следующие наиболее важные формы информации и технических опасностей, которые связаны с достижениями научно-технического прогресса в контексте глобализации:

- Первая форма связана с быстрым развитием нового класса оружия - информации, которая может эффективно влиять на психику, сознание людей, информационно-техническую инфраструктуру общества и армии.

- Вторая форма связана с использованием современных информационных технологий (мошенничество с электронными деньгами, компьютерное хулиганство и т.д.).

- третья форма связана с использованием современных информационных технологий в политических целях.

Это открывает всю глубину проблемы безопасности информационного общества - как противоречие между огромными возможностями, предоставляемыми новыми информационными технологиями для воздействия на социальную организацию и человеческое сознание, с одной стороны, и угрозами их использования в разрушительных для индивидуума, социальной группы, нации, целей, с другой.

Итак, анализируя сказанное, мы получим определения понятий

---

[12] Немыкина О. И. Теоретический анализ проблем информационной безопасности современного общества Теория и практика общественного развития. 2011. № 1. С. 44.

«безопасность» и «информационная безопасность». Безопасность - это состояние, в котором система сохраняет свои важнейшие свойства, стабильность и функционирование.

Информационная безопасность - это состояние, в котором система сохраняет свою целостность информации, стабильность работы и способность сохранять внутреннюю информацию и способность защищать от вторжений внешней информации.

1.2. Нормативно-правовое регулирование информационной безопасности в Российской Федерации

Традиционно правовое обеспечение информационной безопасности рассматривается в рамках информационного права. Информационное законодательство – одна из самых молодых отраслей законодательства. С возникновением Интернета и развитием общественных отношений по поводу информации у государств возникла необходимость правового регулирования данной сферы общественных отношений, определения информационной политики и её защиты.

Так, на встрече руководителей стран «Большой восьмёрки» в Японии 22 июля 2000 г. была принята Окинавская хартия глобального информационного общества, содержащая положение, в соответствии с которым информационные и телекоммуникационные технологии являются одним из приоритетных факторов, оказывающих влияние на формирование общества XXI века[13].

Принятием хартии страны «Большой восьмёрки» провозгласили основные положения, которые будут осуществлять при формировании и

[13] Окинавская хартия Глобального информационного общества. Принята главами государств и правительств «Группы восьми» 22 июля 2000 года // Дипломатический вестник. – № 8. – 2000.– С. 51-56.

распространении информационного общества.

Информация проникает в различные сферы жизнедеятельности общества и государства и приобретает политические, материальные и стоимостные выражения. С возрастанием роли информации, правовое регулирование в информационной сфере становится одним из приоритетных направлений законотворческого процесса в России, цель которого - обеспечение информационной безопасности государства.

Если до 1995 г. в информационной сфере имелись лишь разрозненные правовые нормы, то сегодня правовая база в этой области содержит огромный массив нормативно-правовых актов, который состоит из законодательных актов Российской Федерации, указов Президента Российской Федерации, постановлений Правительства Российской Федерации, нормативно-правовых актов федеральных органов исполнительной власти, а также субъектов Российской Федерации1.

Конституция Российской Федерации 1993 г.[14] является основным источником права в области обеспечения информационной безопасности в России.

Согласно Конституции Российской Федерации 1993 г.:

1) «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (статья 23);

2) «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» (статья 24);

3) «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом» (статья 29);

---

[14] Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с изм. от 21 марта 2014 г. N 6-ФКЗ) // Российская газета от 25 декабря 1993 г. N 237; Собрание законодательства Российской Федерации. - 2014. - N 31. - ст. 4398.

4) «каждый имеет право на достоверную информацию о состоянии окружающей среды» (статья 42)2.

В 1995 г. был принят Федеральный закон Российской Федерации «Об информации, информатизации и защите информации», который являлся основополагающим законодательным актом в России в конце XX – начале XXI веков и регулировал отношения в информационной сфере (в том числе связанные с защитой информации). В Законе были отражены вопросы, связанные с порядком обращения с персональными данными, сертификацией информационных систем, технологий, средств их обеспечения и лицензированием деятельности по формированию и использованию информационных ресурсов.

Позже Федеральный закон 1995 г. был отменен в связи с принятием в 2006 г. Федерального закона Российской Федерации от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»[15]. Как указано в ст. 1: «Настоящий Федеральный закон регулирует отношения, возникающие при: 1) осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации».

В российском обществе сложился государственный, нормативно-правовой подход к понятию информационной безопасности. Информационная безопасность определяется как состояние защищенности информационной среды. Этот вид безопасности рассматривается как составляющая национальной и государственной безопасности.

В 1995 г. был принят Федеральный закон Российской Федерации от 03.04.1995 г. № 40-ФЗ «О Федеральной службе безопасности»[16]. В данном Законе закреплено, что «Федеральная служба безопасности – единая

[15] Федерального закона Российской Федерации от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации» (31 декабря 2017 г.) // СЗ РФ. – 2006. - №31 (Часть I). – Ст. 3448; Справочно-правовая система Гарант.

[16] Федеральный закон Российской Федерации от 03.04.1995 г. № 40-ФЗ «О Федеральной службе безопасности» (с изм. от 18 июня 2017 г. №127-ФЗ) // СЗ РФ. – 2017. - №25. – Ст. 3596.

централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности Российской Федерации».

Обеспечение информационной безопасности является одним из видов деятельности органов Федеральной службы безопасности, осуществляемых ими в пределах их полномочий:

1) при формировании и реализации государственной и научно-технической политики в области информационной безопасности, в том числе с использованием инженерных и криптографических средств;

2) предоставление криптографических и инженерно-технических методов обеспечения безопасности информационных и телекоммуникационных систем, сетей связи специального назначения и других сетей связи, обеспечивающих передачу зашифрованной информации в Российской Федерации и ее учреждениях, расположенных за пределами Российской Федерации "[17].

Постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 была утверждена государственная программа Российской Федерации «Информационное общество (2011-2020 годы)»[18].

Данная Программа включает в себя следующие подпрограммы: 1) «Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на её основе»; 2) «Информационная среда»; 3) «Безопасность в информационном обществе»; 4) «Информационное государство»; а также 5) федеральная целевая программа «Развитие телерадиовещания в Российской Федерации на 2009-2015 годы».

Все подпрограммы, за исключением последней состоят из двух этапов: первый этап рассчитан на 2011-2014 гг., второй этап – на 2015-2020 гг.

В приложениях к данной Программе по многим показателям можно

---

[17] Федеральный закон Российской Федерации от 03.04.1995 г. № 40-ФЗ «О Федеральной службе безопасности» (с изм. от 18 июня 2017 г. №127-ФЗ) // СЗ РФ. – 2017. - №25. – Ст. 3596.

[18] Постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011-2020 годы)» (с изм. от 15 ноября 2017 г. №1384). // СЗ РФ. – 2017. - №47. – Ст. 7007.

определить предполагаемую динамику становление и развитие информационного общества в Российской Федерации.

Так, согласно Приложению № 1 запланировано, какое место будет занимать Российская Федерация в международном рейтинге по индексу развития информационных технологий: 2010-2012 гг. – 48 место, 2013 г. – в числе 40 ведущих стран, 2015 г. – в числе 20 ведущих стран, 2016-2020 гг. – в числе 10 ведущих стран.

Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 была утверждена «Стратегия национальной безопасности Российской Федерации»[19]. Стратегия является основным документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны в долгосрочной перспективе.

Стратегия направлена на консолидацию усилий федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации (далее - государственных органов), органов местного самоуправления, институтов гражданского общества для создания благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации. Федерация.

Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

Стратегия основана на неразрывной взаимосвязи и взаимозависимости национальной безопасности Российской Федерации и социально-

[19] Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. – 2016. - №1 (Часть II). – Ст. 212.

экономического развития страны.

5 декабря 2016 г. Президент Российской Федерации утвердил Доктрину информационной безопасности Российской Федерации. Доктрина представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации[20].

Определены стратегические цели и основные направления обеспечения информационной безопасности.

Анализируются основные информационные угрозы. Оценивается состояние информационной безопасности.

Отмечается, что практика внедрения информационных технологий, не связывая ее с информационной безопасностью, значительно увеличивает вероятность информационных угроз.

На состояние информационной безопасности влияет, в частности, тот факт, что некоторые зарубежные страны расширяют возможности информационного и технического воздействия на информационную инфраструктуру в военных целях. Усиление активности организаций, занимающихся технической разведкой в отношении российских государственных органов, научных организаций и предприятий военно-промышленного комплекса.

Существует тенденция к увеличению объема материалов в зарубежных СМИ с предвзятой оценкой внутренней государственной политики. Российские СМИ часто подвергаются прямой дискриминации за рубежом.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия. Масштабы компьютерной преступности растут.

Приводятся основные направления обеспечения информационной

[20] Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” // Собрание законодательства Российской Федерации. – 2016. - №50. – Ст. 7074.

безопасности в области обороны, государственной и общественной безопасности, в экономической сфере, в науке, технике и образовании, в стратегической стабильности и в равном стратегическом партнерстве.

Состав системы информационной безопасности определяется Президентом Российской Федерации. Совет Безопасности России устанавливает перечень приоритетных областей обеспечения информационной безопасности в среднесрочной перспективе.

Результаты мониторинга реализации доктрины отражены в ежегодном докладе Секретаря Совета Безопасности Президенту Российской Федерации.

В частности, в области развития индустрии информационно-коммуникационных технологий задачи повышения конкурентоспособности российской продукции, создания условий для ее широкого использования при создании отечественных информационных систем и сетей связи и технических средств обеспечения информационной безопасности объектов национальной информационной инфраструктуры выходят на первый план.

Таким образом, можно сделать вывод, что в начале 1990-х годов, когда законодательство в области информационных, информационных и телекоммуникационных технологий только формировалось, главная задача заключалась в его создании, но в настоящее время начался еще один этап развития.

Теперь, когда массив законодательства в этой области достаточно велик, настало время отказаться от количественного роста и перейти к качественной трансформации. Это тем более важно, что за время существования и применения законодательства в области информационных, информационных и телекоммуникационных технологий, упущений и ошибок в разработке соответствующих законодательных актов были выявлены ошибки, которые имеют негативные последствия.

Несмотря на интенсивное развитие законодательства в сфере информационных, информационных и телекоммуникационных технологий, по-

прежнему остается нерешенным значительное количество проблем, и, как показала практика, для некоторых вопросов требуются значительные корректировки уже принятых правовых актов.

1.3. Роль ОВД в обеспечении информационной безопасности РФ

В 1986 году обеспечить электронную безопасность правоохранительных органов, бороться с непреднамеренными радиопомехами, выявлять и предоставлять безобидные специальные технические устройства, предназначенные (спроектированные, адаптированные, запрограммированные) для тайного получения информации, для предотвращения попыток проникновения в компьютерные сети и другие незаконные действия в системе МВД СССР создал новую службу - Отдел электронной войны (EW), более известный как «R» Management. В те годы Бюро «Р» решило чисто оперативные (но не оперативно) следственные задачи, поскольку в соответствии с действующим законодательством тех лет не было компьютерных преступлений. «De jure» они не были, но «де-факто» они были совершены в течение семи лет. Первое компьютерное преступление, официально зарегистрированное Международной организацией уголовной полиции «Интерпол», было совершено в СССР в 1979 году в городе Вильнюсе[21].

Почтовый оператор N. путем мошенничества с использованием автоматизированного программного и аппаратного комплекса «Онега» в течение двух лет совершал хищение средств, направляемых соответствующими государственными органами гражданам в виде пенсий и пособий по старости.

[21] Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014. – С. 11.

Одновременно с компьютерным был проведен обычный (ручной) учет и обработка бумажных (дублированных) учетных документов. Несовершенство программного обеспечения Онеги и наличие двукратной бухгалтерской отчетности, проводимой на различных носителях (в соответствии с формой представления информации), позволяло преступнику в течение длительного времени создавать излишки подотчетных средств, вывести их из кассового аппарата и назначать их, а также уклоняться от ответственности.

1985 год. На Ленинградской верфи была выявлена преступная группа из более чем 70 человек, в которую вошли сотрудники бухгалтерии центрального бухгалтерского отдела завода, должностные лица и материально ответственные лица почти всех структурных подразделений предприятия, возглавляемые руководителем бюро поселений. В период 1981-1985 годов. преступников похитили и присвоили более 200 тысяч рублей.

До 1988 года преступные группы подвергались воздействию, которые действовали аналогичным образом, и совершали хищение в больших и особенно больших количествах на Петровском и Красном Сормовских заводах в Горках (Нижний Новгород), Равенстве в Ленинграде (Санкт-Петербург) и ряде других городов.

Один из характерных исторических примеров - действия организованных преступных групп - уголовное дело о присвоении 125,5 тысяч долларов США и подготовка к краже более чем 500 тысяч долларов во Внешэкономбанке СССР в 1991 году, рассмотренном Московским судом. Согласно материалам другого уголовного дела, в сентябре 1993 года была предпринята попытка украсть деньги в особо крупных размерах из Центрального расчетно-кассового центра Центрального банка России для Москвы на сумму 68 млрд 309 млн 768 тыс. рублей. Те же факты имели место: в апреле 1994 года из центра расчета наличных денег (РКЦ) Махачкалы в размере 1 млн. 557 тыс. Рублей; в Московском филиале «Инкомбанка»; в филиалах Юникомбанка; в коммерческом банке Красноярского края, где было похищено 510 миллионов

рублей; в акционерном коммерческом банке Волгограда - 450 миллионов рублей; в Сбербанке Волгограда - 2 миллиарда рублей.[22]

В 1993-1996 годах было предпринято более 300 попыток проникнуть только в одну компьютерную сеть Центрального банка. В июне 1993 года был зафиксирован факт несанкционированного доступа к автоматизированной системе Главного управления Банка России, сопровождаемый уничтожением части информации о взаимных расчетах.

Август 1994 года. Группа лиц, использующих компьютерную сеть «Искра», внес изменения в программы банка, похитила около 150 тыс. Долларов США в Мытищинском филиале «Юникомбанка».

Июль 1996 года, Ленинградский филиал Сбербанка Калининграда. Неопознанные лица, используя систему международных денежных переводов Western Union, несанкционированно входили в банковскую систему извне, делали произвольные записи в размере 100 тысяч долларов США и снимали необходимые для их передачи и обналичивания реквизиты.

В 1995 году было зарегистрировано более 500 случаев незаконного использования пластиковых кредитных карт (ущерб составил 7 млн. Долл. США, было возбуждено 42 уголовных дела, а в 1996 году - 40 дел). По уровню преступлений такого типа Россия уже к тому времени обогнала западные страны.

В 1997 году, в связи с принятием Уголовного кодекса Российской Федерации и установлением уголовной ответственности за преступления в области компьютерной информации (глава 28), а также других видов компьютерных преступлений, Бюро «Р» учитывая статус оперативных запросов[23].

В то же время существующая численность персонала и материально-

---

[22] Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014. – С. 12.
[23] Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014. – С. 13.

техническая поддержка этого подразделения не позволили ему полностью решить многозадачные задачи. Эта ситуация еще более усугубляется тем фактом, что одновременно с новым Уголовным кодексом Российской Федерации, который начал действовать 1 января 1997 года, были внесены многочисленные поправки в старый Уголовно-процессуальный кодекс РСФСР (1964 г.), который продолжал действуют до конца 2001 года. Поправки касались также расследования преступлений, раскрытие и расследование которых по старому Уголовному кодексу РСФСР было прерогативой федеральной службы безопасности, которая находилась в состоянии постоянной реорганизации. Кроме того, Управлению «R» было поручено (помимо существующих) дополнительные обязанности по обеспечению функционирования Системы оперативной детективной деятельности (SORM), действующей в сетях электросвязи с 1994 года.[24]

Принимая во внимание социально-политическую ситуацию, объективно и субъективно сложившуюся в то время, 7 октября 1998 года офис «Р» был преобразован в Управление по борьбе с высокотехнологичной преступностью (аббревиатура UBPSVT). В его структуре были разделены три группы:

1) отдел по борьбе с преступлениями в области компьютерной информации;

2) отдел по борьбе с преступлениями в области телекоммуникаций;

3) Департамент по борьбе с незаконным оборотом в радиоэлектронных (ВИЭ) и специальных технических средствах (СТС).

В 81 субъекте Российской Федерации, на уровне республиканской, основной и провинциальной МВД, ГУВД и УВД, были созданы аналогичные структурные подразделения - отделы БПЦВТ с тремя филиалами. Первоначально их персонал состоял в основном из оперативного персонала, имевшего техническое образование, что отрицательно сказалось на качестве

[24] Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014. – С. 13.

раскрытия и расследования компьютерных преступлений. По сути, ситуация изменилась к лучшему только к 2000 году, когда подразделения на местах были полностью укомплектованы лицами с высшим и средним специальным юридическим образованием.

В 1999 году в соответствии с постановлением Правительства Российской Федерации № 1701-р от 22.10.99 «Об усилении борьбы с высокотехнологичной преступностью и выполнением международных соглашений и обязательств Российской Федерации» бюджетные средства были немедленно перераспределены всем правоохранительным органам для борьбы с преступностью в рамках соответствующей федеральной программы. Эти деньги были отправлены «... для усиления борьбы с преступлениями в области компьютерной информации и нарушений, связанных с использованием электронных компьютеров, их систем и сетей». Одновременно всем правоохранительным органам было приказано провести разъяснительную и профилактическую работу с населением в этом направлении, которое активно осуществлялось через средства массовой информации.

В соответствии с этим приказом были организованы и проведены различные международные семинары и конференции по борьбе с компьютерными преступлениями, было налажено взаимодействие со спецслужбами зарубежных стран. Результатом всех отмеченных событий стало достижение новых, более качественных и высокоуровневых контрмер против компьютерной преступности как в России, так и на международном уровне.

В 2002 году Управление BPSVT было упразднено, а его персонал, структура и материально-техническое обеспечение были переданы в Бюро специальных технических мер (БСТМ) при Министерстве внутренних дел России. В настоящее время эти подразделения называются департаментами «К» (для борьбы с компьютерной преступностью). Они сохранили специализированные отделы в трех областях борьбы с компьютерной преступностью:

1) отдел по борьбе с преступлениями в области компьютерной информации;

2) филиал по борьбе с преступлениями в области телекоммуникаций;

3) Департамент по борьбе с незаконным оборотом радиоэлектронных (ВИЭ) и специальных технических средств (СТС)[25].

Наряду с Отделами «К» в структуре Главного управления по борьбе с экономическими преступлениями (ГУБЭП) МВД России в субъектах Российской Федерации с 1997 г. были созданы специализированные подразделения – Отделы по борьбе с преступлениями в сфере экономики и компьютерной информации. Они как специализированный орган дознания в силу своей компетенции, регламентированной действующим законодательством, осуществляют выявление, пресечение и предварительное расследование хищений, совершаемых с использованием электронных документов, мошенничеств с кредитными либо расчетными картами, а также незаконного использования объектов авторского права и смежных прав, находящихся на машинных носителях.

В том же 1997 г. в подразделениях Следственного комитета при МВД России, функционирующих при МВД, ГУВД и УВД субъектов Российской Федерации, создаются специализированные следственные отделы и отделения по расследованию преступлений в сфере экономики и компьютерной информации. Следователи органов внутренних дел, входящие в состав таких подразделений, тесно взаимодействуют со специализированными органами дознания – Отделами «К» и ОБЭП.

На данный момент к функциям и задачам подразделения «К» относятся:

1. Борьба с преступлениями в телекоммуникационных сетях:

- с радиоэлектронными устройствами-»двойниками»;

- незаконными междугородними и международными переговорными

[25] Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014. – С. 15.

пунктами, работающими в режиме подмены абонентского номера.

2. Выявление и пресечение преступлений, связанных с осуществлением электронных платежей в телекоммуникационных сетях, в том числе с использованием пластиковых карт.

3. Борьба с незаконным оборотом радиоэлектронных средств (РЭС) и специальных технических средств (СТС), в т.ч. выявление и пресечение каналов их контрабандного ввоза, незаконного изготовления, сбыта и использования.

4. Организация и осуществление радиоэлектронного противодействия незаконно действующим РЭС и СТС.

5. Ведение мониторинга открытых глобальных и локальных компьютерных сетей, сетей проводной, спутниковой и подвижной радиосвязи, а также персонального радиовызова абонента (пейджинга) общего пользования с целью добывания информации о правонарушениях и правонарушителях.

6. Борьба с незаконным оборотом объектов интеллектуальной собственности на электронных (машинных) носителях.

7. Борьба с преступлениями в сфере компьютерной информации, то есть:

- неправомерным доступом к охраняемой законом (конфиденциальной) компьютерной информации (ст. 272 УК РФ);

- созданием, использованием и распространением вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК РФ);

- нарушением правил эксплуатации ЭВМ, систем ЭВМ или их сетей (ст. 274 УК РФ).

В современных условиях информационная безопасность общества, государства и личности является, наряду с другими видами безопасности, включая экономическую, важнейшей составляющей национальной безопасности.

Угрозы информационной безопасности страны, источниками которых являются современные национальные и транснациональные преступные

сообщества, которые охватывают по своей совокупности и масштабам воздействия всю территорию страны и затрагивают все сферы жизнедеятельности общества, подрывают основы национальной безопасности Российской Федерации, нанося ей значительный ущерб.

Органы внутренних дел МВД России являются важной составляющей сил и средств противодействия информационным посягательствам криминальных сообществ на права и свободы граждан, безопасность государства, общества и личности.

В условиях современного состояния преступности, которая в своей основе является масштабной и организованной, охватывает целые регионы и даже всю территорию страны, выходя за ее пределы, имеет большие возможности по доступу к информационным средствам и оружию, их наращиванию и использованию в своей противоправной деятельности, невозможно обеспечить информационную безопасность органов внутренних дел только на основе применения защитных средств и механизмов. В этих условиях необходимо вести активные наступательные (боевые) действия с использованием всех видов информационного оружия и других наступательных средств в целях обеспечения превосходства над преступностью в информационной сфере.

Органы внутренних дел МВД России находятся в состоянии информационной войны как с национальными, так и транснациональными преступными сообществами, специфическим содержанием и основной формой ведения которой являются информационная борьба с использованием информационно-вычислительных и радиосредств, средств радиотехнической разведки, информационно-телекоммуникационных систем, включая каналы космической связи, геоинформационных систем и иных информационных систем, комплексов и средств.

ГЛАВА II. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

2.1. Защита информации как обеспечение информационной безопасности и безопасности информации

В процессе осуществления своей деятельности сотрудники органов внутренних дел получают информацию о режиме и характере работы предприятий, расположенных на обслуживаемой территории, информацию о личной жизни граждан, а также другую информацию (например, официальный характер). Эта информация, а также информация о некоторых методах и результатах работы органов внутренних дел составляют официальную тайну. Раскрытие такой информации, а также утечка информации о мерах, запланированных и проводимых органами внутренних дел по защите общественного порядка и борьбе с преступностью, нарушают их нормальную деятельность и значительно уменьшают ее эффективность.

Возможность хранить конфиденциальную секретную информацию является наиболее важным профессиональным качеством сотрудников правоохранительных органов, что необходимо для успешного выполнения стоящих перед ними задач. В то же время высокий уровень бдительности считается юридическим обязательством сотрудников органов внутренних дел, закрепленных в законодательных и ведомственных нормативных актах. Однако некоторые сотрудники часто недооценивают риск утечки такой информации. Они проявляют беспечность, граничащую с преступной халатностью при рассмотрении официальных документов, что часто приводит к их утрате и раскрытию официальной информации.

На сегодняшний день Министерство внутренних дел России придает большое значение мерам по защите официальной информации. Однако все

существующие недостатки в работе сотрудников ОВД, а также отсутствие необходимой правовой базы, которая обеспечивала бы надлежащую защиту конфиденциальной информации официального характера, не позволяют реализовать механизм для устранения существующих нарушений и привлечения ответственных за нарушения. И это в то время, когда приоритетными областями для развития информационной поддержки системы МВД России, где необходимо применять меры по защите конфиденциальной информации официального характера, являются[26]:

- разработка единых правовых, методических, программно-технических и технологических подходов в организации информационной поддержки правоохранительных органов;

- формирование интегрированных банков данных для коллективного использования оперативной поисковой и справочной информации на основе современных компьютерных технологий с организацией быстрого (не более одной минуты) доступа к ним непосредственно с рабочего места;

- создание единой технологической схемы локальных компьютерных сетей в службах и подразделениях органов внутренних дел с их интеграцией в региональные информационные и компьютерные сети.

Специалистам Министерства внутренних дел Российской Федерации поручено завершить формирование единой методологии сбора, обработки, хранения и защиты оперативного поиска справочной, судебной и статистической информации, а также ввести новые методы работы с информацией поэтапно в течение короткого периода времени. Для завершения перехода на безбумажные технологии сбора, обработки, хранения и передачи официальной информации для обеспечения удаленного доступа к базам данных и банкам публичных данных, а также к федеральным счетам с терминалов, установленных в органах и отделах Министерства внутренних дел Россия,

[26] Швецов А.В. Административно-правовое регулирование служебной тайны / А.В. Швецов, Т.М. Занина II IV Всероссийская научно-практическая конференция «Охрана, безопасность и связь»: Сборник материалов. Часть 2. - Воронеж: Воронежский институт МВД России, 2013. – С. 77.

создать единую ведомственную информационную сеть[27].

В планы Министерства внутренних дел Российской Федерации входят: разработка новых и совершенствование существующего стандартного программного обеспечения и технических решений для компьютеризации системы МВД России; завершение технического перевооружения информационных центров Министерства внутренних дел, Главного управления внутренних дел, УВД; оснащение правоохранительных органов современными средствами компьютерной техники; создание единой автоматизированной технологии для обработки фамилий и отпечатков пальцев федерального и регионального уровней; ввод в действие федерального интегрированного банка данных файла фамилии и оперативно-розыскных записей; обеспечение необходимости выпуска автоматизированных информационных систем органов внутренних дел для внешних автоматизированных информационных систем.

Органами, защищающими государственную тайну, являются: межведомственная комиссия по защите государственной тайны; федеральный орган исполнительной власти, уполномоченный в области безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области иностранной разведки, федеральный орган исполнительной власти, уполномоченный противодействовать технической разведке и технической защите информации, а также территориальные органы; органы государственной власти, предприятий, учреждений и организаций и их структурных подразделений для защиты государственной тайны[28].

Защита государственной тайны является одним из видов деятельности государственного органа, предприятия, учреждения или организации.

Учитывая, что в настоящее время уровень предотвращения

---

[27] Швецов А.В. Формирование института служебной тайны на современном этапе / А.В. Швецов, Т.М. Занина И Всероссийская научно-практическая конференция «Государство, право, общество: современное состояние и проблемы развития». - Липецк: Липецкий филиал Воронежского института МВД России, 2013. – С. 56.

[28] Швецов А.В. Свойства и признаки, отличающие служебную тайну от других видов тайн / А.В. Швецов // Вестник Воронежского института МВД России. - Воронеж: ВИ МВД России. -№. 5 (24). 2005.

дисциплинарных мер защиты служебных секретов не слишком высок, разработка административных и правовых мер по защите такой информации, в которой административные санкции играют важную роль, имеет особое значение. В этом контексте следует отметить, что в специальной части Кодекса об административных правонарушениях Российской Федерации[29] нормы, устанавливающие ответственность за правонарушения в сфере официальной тайны, не имеют признака согласованности и не могут адекватно заполнить правовой вакуум, созданный сужением юридического воздействия уголовных санкций и неэффективности (а в некоторых случаях и отсутствия возможности) применения дисциплинарных санкций.

Привлекая правовую систему защиты служебных секретов, трудно обойтись без уголовно-правовых мер. Хотя в прямом заявлении нет уголовной ответственности за незаконное обращение с информацией, составляющей официальную тайну, ряд существующих преступлений в настоящее время влияет на информацию, охватываемую этой категорией ограничений доступа так или иначе. К уголовно-правовой защите служебных секретов в органах внутренних дел были направлены следующие преступления: «Разглашение данных предварительного расследования» (статья 310), «Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса» (статья 311), «Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа» (статья 320). В целом наказание за такой акт, как раскрытие служебных секретов, полученных при осуществлении полномочий сотрудником органов внутренних дел, может иметь место в рамках преступления «Злоупотребление служебными полномочиями» (статья 285). Однако для судебного преследования в соответствии с настоящей статьей необходимы такие квалифицирующие

[29] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (с изм. от 31.12.2017 г. №499-ФЗ) // Российская газета от 31 декабря 2001 г. №256; Справочно-правовая система Гарант.

признаки, как личные интересы, а также значительное нарушение прав и законных интересов граждан или организаций или интересов общества или государства. Указанная структура распространяется только на категорию должностных лиц, в том числе сотрудников органов внутренних дел, которые в связи с исполнением возложенных на них обязанностей являются носителями служебных секретов.

Как показывает практика правоохранительных органов последних лет, вышеупомянутые составы не в полной мере обеспечивают защиту официальной тайны в деятельности правоохранительных органов. Эта ситуация, по нашему мнению, объясняется тем, что в нормах действующего уголовного законодательства нет систематического подхода к формированию защиты официальных секретов. Предоставление этим категориям информации статуса официальных секретов и введение отдельной статьи для ее раскрытия и других незаконных действий позволило бы исключить из Уголовного кодекса Российской Федерации во многих отношениях совпадающие композиции и определить ответственность. Для достижения этой цели мы на основе анализа вышеупомянутых преступлений предлагаем свое концептуальное видение решения проблемы комплексной защиты служебных секретов, когда правоохранительные органы выступают в качестве одного из участников уголовного права связи.

Защита служебных секретов в деятельности ОВД нормами уголовного права следует рассматривать в следующих аспектах:

- когда сами сотрудники ОВД выступают в качестве субъектов преступления в связи с совершением ими противоправного деяния с информацией, которая содержит официальную тайну, полученную при исполнении служебных полномочий;

- когда должностные лица ОВД обязаны принимать законные меры для пресечения незаконного действия информацией, содержащей официальную тайну, полученную лицом, имеющим доступ к нему на законных основаниях.

Рассмотрение этих аспектов проблемы должно проводиться взаимосвязано, поскольку именно этот порядок позволяет в комплексе обеспечить уголовно-правовую защиту служебных секретов в органах внутренних дел. Наличие в Уголовном кодексе формулировок, направленных на защиту служебных секретов, не позволяет сегодня говорить о какой-либо полноте, они не полностью отражают реальное положение вещей в этой области.

Из основных задач органов внутренних дел наиболее информативными являются:

- предупреждение и пресечение преступлений и административных правонарушений;

- выявление и раскрытие преступлений.

При решении этих задач органы внутренних дел аккумулируют огромное количество разнородной информации, включая ограниченную информацию, составляющую государственную тайну, и другую конфиденциальную информацию.

Они включают личные данные о гражданах и информацию, составляющую коммерческую, профессиональную тайну хозяйствующих субъектов и другую деятельность, а также информацию, составляющую государственную тайну, касающуюся специфики деятельности предприятий оборонного комплекса, воинских частей и других субъектов.

Отдельно необходимо остановиться на информации о состоянии внешней среды, которую органы внутренних дел по праву получают в результате оперативно-розыскной деятельности. Наиболее информативным с точки зрения процента информации ограниченного распространения является деятельность, связанная с информированием органов внутренних дел лицами, сотрудничающими с ними на конфиденциальной основе, а также сотрудниками органов внутренних дел, которые оперативно внедряются в организацию, в отношении которых имеются реалистичные предположения о том, что они занимаются преступной деятельностью.

Существенный приток информации ограниченного распространения в органы внутренних дел также обеспечивается такой оперативно-розыскной деятельностью, как запрос, наблюдение, осмотр помещений, зданий, сооружений, удаление информации из технических каналов связи, прослушивание телефонных разговоров, проводимых в процессе обнаружения, раскрытия и пресечение преступлений. Значительные объемы информации ограниченного распространения органам внутренних дел также предоставляются официальной перепиской, которую они осуществляют с другими государственными органами, государственными и неправительственными организациями и учреждениями. Конкретным свойством этой информации является то, что степень их секретности (конфиденциальности), содержащейся в документах, чаще всего заранее определяется отправителем. Однако, если это правило безоговорочно выполняется в отношении информации, составляющей государственную тайну, то в отношении личных данных, коммерческой тайны хозяйствующих субъектов, отправители документов не всегда могут адекватно оценивать уровень их конфиденциальности, а чаще всего информация попадает в органы внутренних дел в потоке общей открытой переписки.

Значительный объем информации ограниченного распространения накапливается органами внутренних дел также во время предварительного расследования по уголовным делам.

Следует также отметить, что часть информации, поступающей из внешней среды, независимо от ее содержимого, автоматически классифицируется. Это связано с каналом для получения такой информации (конфиденциальные источники). Однако в общем потоке поступающей информации они занимают небольшую часть.

Закон Российской Федерации «О государственной тайне»[30] как основной

[30] Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (с изм. от 26.07.2017 № 193-ФЗ) // Российская газета. – 21 сентября 1993. - №182; от 31 июля 2017 г. №167.

источник норм, регулирующих отношения в этой области, предусматривает, что деятельность по защите этой категории информации осуществляется специализированными подразделениями государственных органов (подразделениями по защите государственной тайны). Такую роль в органах внутренних дел выполняют секретариаты (отделения), подразделения криптографической службы и подразделения по противодействию технической разведке.

Каждое из этих подразделений выполняет ограниченную функцию для обеспечения защиты информации, составляющей государственные секреты:

- секретариаты (отделения) - обеспечивают оборот документов, их хранение и уничтожение, а также контроль за правильностью обращения таких документов в органах внутренних дел;

- подразделения криптографической службы - обеспечивают криптографическую защиту информации, передаваемой по каналам связи, а также учет и хранение документов, передаваемых по каналам связи;

- подразделения для противодействия технической разведке - обеспечивают реализацию комплекса мер, направленных на исключение возможности утечки информации по так называемым «боковым» каналам (энергетические сети, радиопередача и т.д.).

Правильная формулировка вопроса о внедрении комплекса мер по обеспечению защиты информации, составляющей государственную тайну, требует очень точной координации оперативной и официальной деятельности вышеуказанных подразделений друг с другом для достижения главной цели - обеспечения безусловной безопасности информации от незаконного распространения. Однако при решении этой проблемы в системе МВД России существуют традиционные проблемы, а именно, что вышеупомянутые подразделения находятся в разных службах и не связаны с администрацией друг с другом.

Между тем создание единой структуры, которая могла бы формулировать

и осуществлять политику защиты информации, составляющей государственную тайну в органах внутренних дел на нынешнем этапе, еще более актуальна, чем раньше. В советский период система Министерства внутренних дел, несмотря на внешние атрибуты (присутствие министерств внутренних дел в союзных и автономных республиках), почти полностью управлялась из единого центра - Союза республиканских министерств внутренних дел СССР. В этих условиях осуществление общей политики по организации и осуществлению режима секретности в оперативной и официальной деятельности органов внутренних дел было не очень сложным, поскольку как руководящие документы, так и вспомогательная поддержка поступали из единого центра, он также осуществлял ведомственный контроль за состоянием этой деятельности.

В настоящее время существенно расширилась независимость региональных органов внутренних дел, финансирование их деятельности осуществляется, помимо прочего, за счет бюджетов субъектов Российской Федерации и местных бюджетов, что в некоторых случаях позволяет обеспечить адекватный уровень финансирования программ, осуществляемых из-за неравного состояния экономики в разных регионах. Более того, предстоящая реформа системы органов внутренних дел предусматривает их разделение на федеральный компонент (криминальная полиция) и региональный компонент (полиция общественной безопасности), что может вызвать дополнительный дисбаланс в уровне обеспечения государственной тайны.

Исходя из вышесказанного, мы считаем, что способность эффективно решать проблемы безопасности информации, составляющей государственную тайну в органах внутренних дел, будет в значительной степени зависеть от формирования единой службы, которая будет отвечать за весь спектр мер для защиты информации в своей деятельности.

2.2. Ответственность за совершение информационных и компьютерных преступлений

Современное развитие технологий и Глобальной сети наряду с преимуществами, выражающимися в доступности информации образовательного характера и беспрепятственном коммуникационном взаимодействии, породило необычайно широкие возможности для преступной деятельности. Неустанный рост преступлений представленного направления в России обусловлен различными причинами, среди которых, во-первых, необходимо назвать стабильно высокий количественный показатель российской интернет-аудитории. Таким образом, ежемесячная аудитория интернет-пространства в Российской Федерации в 2017 году достигла 87 миллионов человек, что составляет 71% от общей численности населения страны[31]. В связи с этим, выявление проблем, связанных с преступлениями в сфере компьютерной информации, а также совершенствование законодательства в данной области, - представляются разумными задачами.

Следует обозначить, что ответственность за преступления в сфере компьютерной информации российский законодатель регламентировал в положениях главы 28 Уголовного кодекса Российской Федерации, которая вобрала в свой состав всего три статьи - «Неправомерный доступ к компьютерной информации», «Создание, использование и распространение вредоносных компьютерных программ» и «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»[32]. Нет других правил, которые предусматривали бы ответственность за незаконные действия в области

[31] Количество пользователей интернета в России // Интернет в России и в мире [Электронный ресурс]. - Режим доступа: http://www.bizhit.ru/ index/users_count/0-151.

[32] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изм. от 19 февраля 2018 г. №25-ФЗ) // Собрание законодательства Российской Федерации. – 1996. - №25. – Ст. 2954; Справочно-правовая система Гарант.

компьютерной информации. Очевидно, что при таком небольшом объеме правового регулирования в представленной области сплошной слой вопросов оставался без должного внимания.

Необходимо понимать, что положительная динамика сферы компьютерной информации оказывает определенное влияние как на ее непосредственные компоненты, так и на действия, которые косвенно затрагивают определенные аспекты такой области. То есть наряду с развитием информационных технологий формируются, изменяются и развиваются новые формы и формы преступности, что в свою очередь оказывает непосредственное влияние на концептуальный аппарат и сложность квалификации преступных деяний.

Предметом преступлений представленной сферы является информация, которая хранится и обрабатывается в компьютерных системах. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» под информацией подразумеваются сведения (сообщения, данные) независимо от формы их представления[33]. Примечание к статье 272 Уголовного кодекса Российской Федерации раскрывает понятие «компьютерная информация». Так, под информацией подобного рода понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[34].

Объектом этой группы преступлений являются общественные отношения, которые обеспечивают безопасность и конфиденциальность компьютерной информации; к необязательному объекту следует включать личные права граждан, права законных владельцев программ для электронных

[33] Федерального закона Российской Федерации от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации» (31 декабря 2017 г.) // СЗ РФ. – 2006. - №31 (Часть I). – Ст. 3448; Справочно-правовая система Гарант.

[34] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изм. от 19 февраля 2018 г. №25-ФЗ) // Собрание законодательства Российской Федерации. – 1996. - №25. – Ст. 2954; Справочно-правовая система Гарант.

компьютеров и баз данных, отношения собственности, а также безопасность общественного и государственного уровней[35].

Статья 272 под заголовком «Неправомерный доступ к компьютерной информации» устанавливает ответственность за незаконный доступ к компьютерной информации, защищенной законом, если этот акт повлек за собой уничтожение, блокирование, модификацию или копирование компьютерной информации. Составные материалы являются материальными. Законодательство не устанавливает определение несанкционированного доступа к компьютерной информации, что порождает определенные трудности в квалификации преступления.

Необходимо понимать, что доступ к компьютерной информации понимается как способность изучать или использовать компьютерную информацию. То есть доступ - это прежде всего производительность определенных действий, которые могут быть выражены в проникновении в компьютерную систему с использованием специальных технических или программных инструментов, которые позволяют вам преодолеть установленные системы защиты, незаконное использование существующих паролей или кодов для входа в компьютер , или выполнять другие действия для проникновения в систему или сеть под видом законного пользователя. Таким образом, доступ к компьютерной информации лица, не имеющего права на получение такой информации и работы с такой информацией или компьютерной системой, в отношении которой были приняты специальные меры защиты, ограничивающие круг лиц, имеющих доступ к ней, признан незаконным.

Российская судебная практика актуализировала проблему отграничения «Неправомерного доступа к компьютерной информации» от «Нарушения авторских и смежных прав». Сложность квалификации обусловлена тем, что в

---

[35] Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ - Scientific Journal of KubSAU. - 2013. - №90 [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/ article/n/problemy-kvalifikatsii-prestupleniy-v-sfere-kompyuternoy-informatsii-1.

некоторых случаях преступник получает доступ к компьютерной программе, которая является объектом авторского права, и использует ее в своих интересах. В таком примере, прежде всего, необходимо установить объект преступления. Итак, если объектом преступления, предусмотренным в статье 272 Уголовного кодекса Российской Федерации, являются общественные отношения в области безопасности и конфиденциальности компьютерной информации, соответственно, нарушения должны нарушать безопасность компьютерной информации, а затем нарушение авторского права и смежных прав ущемляет интеллектуальную собственность. Предметом первого из вышеуказанных преступлений является компьютерная информация, которая защищена законом, а субъект второго - исключительно объекты авторского права. Следует отметить, что объективная сторона нарушения авторского права и смежных прав в качестве необходимой функции включает начало социально-опасных последствий в виде причинения серьезного ущерба автору объекта авторского права в виде упущенной выгоды или морального вреда , Чтобы привлечь виновника к уголовной ответственности в соответствии со статьей «Незаконный доступ к компьютерной информации», эта функция не является обязательной. Также важно, что нарушение авторского права и смежных прав связано либо с атрибуцией авторства, либо с незаконным использованием объектов авторского права, а при наличии несанкционированного доступа к компьютерной информации его дальнейшее использование виновным не является необходимо. Стоит отметить случаи, когда преступник, чтобы передать право автора, копирует компьютерную программу, а воспроизводимые копии незаконно использует в своих преступных интересах. В этом случае преступление, совершенное преступником, подлежит квалификации на основании статей 146 и 272 Уголовного кодекса Российской Федерации, если автор программы подвергся серьезному ущербу[36].

[36] Комментарий к Ст. 272 УК РФ // Уголовный Кодекс Российской Федерации со всеми изменениями и дополнениями. Комментарий к статьям УК РФ [Электронный ресурс]. - Режим доступа: http://stykrf.ru/272.

Статья 273 под заголовком «Создание, использование и распространение вредоносных компьютерных программ» устанавливает ответственность за создание, использование и распространение вредоносных компьютерных программ.

Состав преступления формальный. То есть для признания преступления достаточно установить факт совершения общественно опасного акта, если он создает реальную угрозу создания, использования и распространения вредоносных компьютерных программ.

Стоит отметить, что эта композиция имеет некоторые общие черты с составом преступления «Незаконный доступ к компьютерной информации». Трудность в выявлении этих преступлений заключается в том, что незаконный доступ к компьютерной информации, а также создание, использование и распространение вредоносных компьютерных программ приводят к несанкционированному уничтожению, блокированию, модификации или копированию информации или нейтрализации средств защиты компьютерной информации[37]. В подобном примере прежде всего необходимо определить предмет преступления. Предметом преступления «Неправомерный доступ к компьютерной информации» является только та информация, которая законодательно подлежит охране. Предметом же преступления «Создание, использование и распространение вредоносных компьютерных программ» является любая информация, которая содержится на машинном носителе или в информационно-телекоммуникационных сетях.

Статья 274 под заголовком «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

[37] Комментарий к Ст. 273 УК РФ // Уголовный Кодекс Российской Федерации со всеми изменениями и дополнениями. Комментарий к статьям УК РФ. [Электронный ресурс]. - Режим доступа: http://stykrf.ru/273.

Соответственно, объективная сторона данного преступления состоит в нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, которое повлекло за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. То есть, необходимым элементом преступления должно быть причинение крупного ущерба. Состав преступления - материальный. Между фактом нарушения и наступившим ущербом должна быть установлена причинная связь. Таким образом, наступившие последствия должны являться результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными иными статьями главы «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации.

Что касается аспекта совершенствования законодательства в представленной сфере, то стоит обозначить, что в уголовно-правовой науке сформировалось два основных направления по решению проблем законодательства в части квалификации преступлений в сфере компьютерной информации.

Согласно первому направлению, в ряд составов («Нарушение авторских и смежных прав», «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», «Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники» и так далее) необходимо ввести такой способ совершения преступления, как «с применением компьютерных средств» (выдвигаются и такие трактовки, как «...с применением компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, системы или сети связи, иных высокотехнологичных и научно-технических средств», «с применением информационных

технологий» и так далее)[38]. Причём представленное направление частично уже апробировано законодателем. Так, в Уголовный кодекс Российской Федерации был внесен новый состав мошенничества - «Мошенничество в сфере компьютерной информации». Данный состав закрепил за собой ответственность за мошенничество в данной сфере, то есть хищение чужого имущества или приобретения права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей. Казалось бы, что типичной формой мошенничества является его совершение с использованием сети Интернет, однако регулирование сферы, касающейся Интернета как компьютерной сети, не носило правового характера и относилось лишь к области технических стандартов[39]. Это при том, что сотрудниками правоохранительных органов был обозначен ряд проблем, которые возникали при квалификации мошенничества в сфере высоких технологий, в котором не задействованы ни ЭВМ, ни система ЭВМ и их сети[40]. То есть, это весьма точное и отвечающее современным реалиям правоприменительного толка нововведение, так как до принятия поправки мошенничество путём неправомерного доступа к компьютерной информации требовало квалификации по совокупности преступлений «Мошенничество» и «Неправомерный доступ к компьютерной информации». То есть, одним действием лицо совершало два преступления. Теперь же достаточно квалификации по статье «Мошенничество в сфере компьютерной информации», что ведёт к логичному упрощению процесса уголовного

[38] Нагорный А.А. Проблемы квалификации преступлений в сфере компьютерной информации // Oaji.net [Электронный ресурс]. - Режим доступа: http://oaji.net/articles/2014/245-1393744181.pdf.
[39] Медведев С.С. Мошенничество в сфере высоких технологий: Дис. ... канд. юрид. наук: 12.00.08 / Медведев Сергей Сергеевич; Кубан. гос. аграр. ун-т. - Краснодар, 2008. – С. 24.
[40] Кондратов М.А. К постановке вопроса об уголовной ответственности юридических лиц в уголовном праве России (исторический аспект) / М.А. Кондратов, С.С. Медведев // Научный журнал КубГАУ - Scientific Journal of KubSAU. - 2015. - №106 [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/article/n/k-postanovke-voprosa-ob-ugolovnoy-otvetstvennosti- yuridicheskih-lits-v-ugolovnom-prave-rossii-istoricheskiy-aspekt.

судопроизводства[41].

Согласно второму направлению, необходимо ввести отдельный раздел в Уголовном кодексе Российской Федерации, который будет полностью посвящен компьютерным преступлениям. Однако, во-первых, в этом случае нарушается системный характер уголовного законодательства. И, во-вторых, вопрос о достоверности перечня компьютерных преступлений до сих пор остается нерешенным.

Поскольку положительно динамическая динамика сферы компьютерной информации оказывает очень заметное влияние на новые типы и формы преступлений, что, в свою очередь, оказывает непосредственное влияние на концептуальный аппарат и сложность квалификации преступных деяний, тогда ответ законодателя должен быть в рабочем состоянии и соответствовать реалиям правоохранительных органов. В российской науке о криминальном праве разработаны два основных курса, направленных на решение проблем законодательства с точки зрения квалификации преступлений в области компьютерной информации. И некоторые из нововведений, полученных на этих курсах, активно используются на практике. Однако специфика сферы компьютерной информации диктует необходимость постоянного всестороннего совершенствования уголовного законодательства.

2.3. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации

Программное обеспечение позволяет изменять и разрабатывать

[41] Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ - Scientific Journal of KubSAU. - 2013. - №90 [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/ article/n/problemy-kvalifikatsii-prestupleniy-v-sfere-kompyuternoy-informatsii-1.

различные программы, которые могут быть отнесены одновременно к преимуществам системы, а также к недостаткам с точки зрения защиты обрабатываемой на ней информации. Здесь есть два противоречия. Во-первых, персональный компьютер характеризуется полной доступностью всех ресурсов. Многие программные продукты имеют свою собственную защиту, но отсутствие как базового набора инструментов для обеспечения безопасности информации, так и систематических политик безопасности значительно снижает эффективность использования отдельных несвязанных продуктов безопасности. Во-вторых, персональный компьютер может работать в многопользовательском режиме, а также использоваться в компьютерных сетях разного масштаба и в круглосуточном режиме, что повышает уязвимость обрабатываемой информации[42].

В связи с тем, что персональный компьютер имеет достаточно высокую стоимость, он может стать объектом криминального нападения.

Современные методы накопления, обработки и передачи информации способствовали возникновению угроз, связанных с возможностью потери, раскрытия, модификации данных, принадлежащих конечным пользователям.

На практике угрозы могут быть реализованы прямым воздействием как на информацию, представляющую интерес для конечных пользователей таких систем, так и на информационных ресурсах и телекоммуникационных услугах, которые обеспечивают обмен информацией в рамках информационной системы.

Угроза информации - потенциально существующая опасность случайного или преднамеренного уничтожения, несанкционированного получения или изменения информации из-за структуры системы обработки и условий обработки и хранения информации в информационной системе[43].

Все угрозы для информации можно разделить на два типа: естественные

---

[42] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 51.
[43] Там же. – С. 51.

и искусственные.

Естественные угрозы информации - это угрозы, вызванные форс-мажорными обстоятельствами, то есть независимыми от человека. К таким угрозам относятся различные стихийные бедствия; разбивка аппаратной части информационной системы; отказ электропитания из-за отказа оборудования или его повреждения при стихийных бедствиях (прерывание линии электропередачи, пробой генератора или электростанции); повреждение каналов связи; сбой программного обеспечения (в случае, если ошибочные действия пользователя не привели к этому).

Следует отметить, что при сбое лицензионного программного обеспечения создатели программного обеспечения должны нести ответственность за потерю информации или потерю качества информации, если иное не предусмотрено лицензионным соглашением. Это не относится к программам, поставляемым «как есть», для последствий использования которых создатель не несет ответственности.

Искусственные угрозы информации называются угрозами, которые возникают в результате человеческой деятельности. В свою очередь, искусственные угрозы, в зависимости от мотивации действий, можно разделить на случайные и преднамеренные.

Случайные угрозы вызваны ошибками, возникшими во время проектирования информационной системы, ошибками пользователей при работе с системой, ошибками, возникающими при работе программного обеспечения. Случайные угрозы включают: ошибки в хранении, передаче и использовании информации; нарушение защиты, ошибки в подготовке и вводе информации, ошибки операционной системы, ошибки программы; аппаратные ошибки, неправильное толкование инструкций, пропуски необходимых операций, нарушение последовательности операций; ошибки в создании информационных систем и ошибки в их реализации; неосторожное хранение и запись носителей информации.

Преднамеренные угрозы связаны с намерением человека уничтожить, незаконно копировать, блокировать или модифицировать информацию или нанести ущерб или уничтожить аппаратное обеспечение информационной системы, программного обеспечения и другого вспомогательного оборудования, которое приведет или может привести к уничтожению, блокированию, модификации информация и т. д. Преднамеренные угрозы включают: несанкционированный доступ; перехват информации с помощью технических средств извлечения информации; перехват информации с помощью программного обеспечения и математическое влияние на обработку информации; подкуп лиц, имеющих доступ к информации; мошенничество, кража, саботаж, шантаж, вымогательство и другие преступления, предметом которых является информация[44].

Перед разработкой систем компьютерной безопасности необходимо оценить все потенциальные угрозы и каналы утечки информации.

Появление возможных каналов преднамеренного несанкционированного доступа к информации зависит от двух факторов: от поддерживаемого режима работы и его конфигурации.

Различать автономный режим работы и сеть - в локальной, региональной или глобальной сети.

В автономном режиме работы возможны два варианта управления компьютером:

1) одиночный пользователь, в котором пользователь сам выполняет функции контроля и мониторинга и несет ответственность за безопасность своей и информации, которой он доверяет;

2) многопользовательский, в котором вышеуказанные функции выполняются специальным лицом. Они могут быть одним из пользователей или менеджером работы. Однако ключи шифрования и информация, закрытые

---

[44] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 52.

другим пользователем, могут быть недоступны до тех пор, пока работа не будет передана супервизору[45].

К компьютеру могут быть подключены различные периферийные устройства - плоттер, сканер, стример, внешние запоминающие устройства, которые образуют дополнительный канал утечки из-за ложного электромагнитного излучения. Значительное влияние на уровень радиации информации оказывает влияние тип монитора.

Анализируя вышеуказанные факторы, мы можем выделить три основные группы каналов утечки:

1) каналы, связанные с работой оборудования,

2) каналы, связанные с функциями программного обеспечения,

3) каналы, связанные с действиями людей (злоумышленники или обслуживающий персонал)[46].

Группа каналов, связанных с работой оборудования:

- подключение специального оборудования и внесение изменений в оборудование;

- использование специальных технических средств для перехвата электромагнитных излучений оборудования и линий связи.

Каналы, связанные с функциями программного обеспечения, включают:

- несанкционированный доступ программ к информации;

- расшифровка программой зашифрованной информации;

- копирование защищенной информации.

Группа каналов, связанных с действиями людей, формирует:

- кража носителей информации (дисководы, гибкие диски, ленты, документация);

- считывание информации с экрана неавторизованным лицом;

- чтение информации из распечаток, оставленных без присмотра;

---

[45] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 53.

[46] Там же.

- ввод заведомо ложной информации;

- копирование ограниченной информации;

- проникновение в компьютерные сети[47].

В качестве основных целей защиты компьютерной информации, обеспечения физической целостности, предотвращения несанкционированного получения, предотвращения несанкционированной модификации, предотвращения несанкционированного копирования.

Физическая целостность компьютерной информации зависит в первую очередь от здоровья самого компьютера и средств массовой информации. В широком диапазоне угроз целостности компьютерной информации выделяются угрозы, связанные с неквалифицированными действиями людей, ведущих к уничтожению или искажению данных.

Предотвращение несанкционированной модификации связано, прежде всего, с предотвращением заражения компьютерными вирусами.

Предотвращение несанкционированного получения информации становится особенно актуальным в случаях, когда информация, обрабатываемая или хранящаяся, является конфиденциальной или содержит секрет другого характера.

Актуальность проблемы предотвращения несанкционированного копирования информации обусловлена следующими факторами: трансформацией электронных массивов информации в товар; распространение программных продуктов на коммерческой основе.

Список основных задач, которые должны быть решены системой компьютерной безопасности:

1) управление доступом к ресурсам для защиты от несанкционированного случайного или преднамеренного вмешательства в работу системы, ее информации, программно-технических ресурсов неавторизованных лиц, а

---

[47] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 53.

также отдельных лиц из числа пользователей;

2) защита данных, передаваемых по каналам связи;

3) регистрация, сбор, хранение, обработка и выдача информации обо всех событиях, происходящих в системе и связанных с безопасностью;

4) контроль работы пользователей системы администрацией и оперативное уведомление администратора безопасности о попытках несанкционированного доступа к системным ресурсам;

5) мониторинг и поддержание целостности критически важных ресурсов системы защиты и среды исполнения прикладных программ;

6) предоставление закрытой среды для проверенного программного обеспечения для защиты от неконтролируемого внедрения в систему потенциально опасных программ (которые могут содержать вредоносные закладки или опасные ошибки) и средства преодоления системы защиты, а также от внедрения и распространения компьютерные вирусы;

7) управление системой защиты[48].

Обычно различают внешнюю и внутреннюю безопасность компьютерных систем. Внешняя безопасность включает защиту от стихийных бедствий (пожар, наводнение и т.д.), от проникновения в систему нарушителей снаружи с целью кражи, получения доступа к информации или выведения системы из строя.

Все усилия по обеспечению внутренней безопасности компьютерных систем направлены на создание надежных и удобных механизмов для регулирования деятельности всех его законных пользователей и обслуживающего персонала, с тем чтобы заставить их безоговорочно соблюдать дисциплину, установленную в организации доступа к системным ресурсам (в том числе Информация). Кроме того, внутренняя безопасность включает в себя обучение пользователей навыкам обязательного тестирования,

[48] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 54.

различных административных действий и т.д.

1. Защита информации от случайных влияний

Случайные последствия для информации в виде сбоев и сбоев в оборудовании, вмешательства со стороны окружающей среды, ошибок разработчиков, пользователей и персонала, аварийных ситуаций являются наиболее реальными угрозами целостности компьютерной информации. Актуальность обеспечения целостности информации не зависит от ее типа, поэтому знания в этой области необходимы всем пользователям.

Для устранения влияния этих негативных факторов используется соответствующее защитное оборудование.

Чтобы уменьшить повреждение целостности информации из-за отказа и отказа оборудования и помех от окружающей среды, используются резервные источники бесперебойного питания, а надежные системы построены из менее надежных элементов из-за их структурной избыточности. Кроме того, используются более надежные детали и компоненты.

Влияние программных, алгоритмических и системно-технических ошибок разработчиков может быть значительно уменьшено за счет применения функциональных средств управления с диагностикой отказа.

Создание системы жизнеобеспечения пользователя приводит к значительному сокращению ошибок с их стороны и, кроме того, позволяет сохранять информацию в случае возникновения чрезвычайной ситуации и других непредвиденных ситуаций.

Для предотвращения или минимизации ущерба, вызванного чрезвычайными ситуациями, необходимо разработать план организационных мероприятий и создать условия для резервного копирования и хранения информации.

2. Защита информации от преднамеренных воздействий

Главная угроза целостности компьютерной информации - это преднамеренные угрозы, которые могут быть прямыми, если злоумышленник

получает доступ к компьютеру и опосредуется, когда угроза создается с использованием промежуточной среды.

Самой серьезной угрозой для защищенной информации является несанкционированный доступ. Мы перечисляем основные средства защиты компьютерной информации:

1) физическая защита компьютера и носителей;

2) идентификация, аутентификация и авторизация пользователей и компонентов системы;

3) разграничение доступа к элементам защищенной информации;

4) регистрация всего доступа к защищенной информации[49].

Физические средства защиты компьютера и носителей. Компьютер лучше всего помещается в надежно запертой комнате, а в рабочее время помещение должно быть закрыто или под наблюдением законного пользователя. При обработке конфиденциальной информации в комнате могут быть только те, у кого есть соответствующее разрешение.

Идентификация и аутентификация пользователей и компонентов системы. Механизмы идентификации, аутентификации и авторизации необходимы для подтверждения подлинности субъекта, обеспечения его работы в системе и определения легитимности прав субъекта на объект или определенных действий с ним.

Идентификация (именование и распознавание) - это процесс распознавания системного элемента, обычно с использованием предопределенного идентификатора или другой уникальной информации; каждый объект или объект системы должен быть однозначно идентифицирован.

Аутентификация (аутентификация) - это аутентификация личности пользователя, процесса, устройства или другого системного компонента

[49] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 54.

(обычно выполняется до доступа), а также проверка целостности и авторства данных при их сохранении или передаче для предотвращения несанкционированной модификации.

Авторизация - это предоставление субъекту прав доступа к объекту.

Объектами идентификации и аутентификации могут быть: лицо (пользователь, оператор, официальное лицо), технические средства (терминал, дисплей, ПК), носители (магнитные ленты, диски, отпечатки, списки), информация на дисплее,

Аутентификацию объекта может выполнять человек, аппаратное устройство, программа или компьютерная система. В настоящее время на практике используются следующие методы аутентификации и аутентификации:

1) система паролей;

2) анализ антропометрических параметров пользователя - голос, походка, лицо, радужная оболочка и сетчатка, отпечатки пальцев или отпечатки пальцев (ДНК не включена в этот список, поскольку выборка его образца медленная и неудобная для человека); электронные ключи[50].

Использование системы паролей состоит в том, что каждый зарегистрированный пользователь имеет личный пароль, который хранится в секрете и запрашивается при доступе к IS. Система паролей характеризуется простотой и низкой стоимостью реализации, с небольшим компьютерным временем и не требует больших объемов памяти. Существующие пароли можно классифицировать по типу.

Простые пароли

Пользователь вводит такой пароль с клавиатуры после запроса, а компьютерная программа (или специальный чип) кодирует ее и сравнивает с сохраненным стандартом. Преимущество простого пароля в том, что его не нужно записывать, а недостатком является то, что он может перехватывать

[50] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 59.

пароль с помощью видеонаблюдения, ключевых ошибок (устройств, которые автоматически сохраняют точную копию того, что набирается на клавиатуре) и т.д. Простой пароль рекомендуется для данных защиты с небольшой стоимостью и стоимостью.

Одноразовые пароли

Пользователю предоставляется список N паролей, которые хранятся в памяти компьютера в зашифрованном виде (также известны варианты списка паролей, которые печатаются на специальных карточках с защитной крышкой). Каждый пароль используется только один раз, поэтому перехват пароля становится бессмысленным. Такой пароль обеспечивает более высокую степень безопасности, но более сложную. У него есть другие недостатки. Во-первых, вам нужно где-то хранить список паролей, так как его почти невозможно запомнить. Во-вторых, после использования всех паролей вам нужно получить новый список. Следует учитывать, что злоумышленник может попытаться перехватить управление сеансом законного пользователя. В этом случае законный пользователь получает сообщение о завершении сеанса, а злоумышленник подключается к сеансу и выполняет необходимые действия от имени законного пользователя[51].

Пароли, основанные на выборке символов

Пользователь вводит с паролем некоторые символы, позиции которых задаются путем преобразования случайных чисел или генератора псевдослучайных чисел. Очевидно, что пароль должен быть достаточно часто изменен, поскольку несанкционированный пользователь может в конечном итоге создать пароль от отдельных символов.

Пароли методом запроса-ответа

Пользователь должен дать правильные ответы на набор вопросов, хранящихся в памяти компьютера и контролируемых операционной системой.

---

[51] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 59.

Иногда пользователю задают много вопросов, и он может выбирать те, на которые он хочет ответить сам. Преимущество этого метода заключается в том, что пользователь может выбирать вопросы, и это дает очень высокую степень безопасности.

Графические пароли

При создании пароля пользователю предлагается выбрать и запомнить десять значков примерно из 200-400 возможных. Если вам нужно ввести пароль, система отобразит огромную панель значков, смешанную случайным образом. Среди них обязательно будет три или четыре «твои». Они должны быть мысленно связаны линиями (получается треугольник или квадрат) и щелкните в любом месте внутри этой фигуры. Сразу же иконки перестраиваются, смешиваются. Одни в то же время исчезают, другие - добавляются. И снова среди всего этого хаоса, который вы видите, и любые ваши собственные значки из самой десятки (не обязательно тех, которые были на экране только сейчас). Предоставляет для создания пароля выбор настроек: количество значков, скорость их перемещения, количество кликов на фигурах и некоторые другие параметры[52].

Основная идея заключается в том, чтобы позволить пользователю доказать знание пароля, не показывая сам пароль в процессе его ввода. Вопрос меняется каждый раз, и ответ тот же. Но «секретные знания» остаются прежними. Даже если вы наберете графический пароль за спиной, появится человек и запомните все ваши действия и клики - он никогда не сможет войти в IS на вашем месте. После просмотра видео с камеры безопасности никто не сможет восстановить ваш пароль. Отсутствие этой системы: для входа в систему требуется гораздо больше времени, чем традиционный набор символов в поле пароля.

Пароли, основанные на алгоритме

---

[52] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 60.

Пароль определяется на основе алгоритма, который хранится в памяти компьютера и известен пользователю. Система отображает случайное число на экране, а пользователь, с одной стороны, и компьютер, с другой стороны, на его основе вычисляют пароль с использованием известного алгоритма. Этот тип пароля обеспечивает более высокую степень безопасности, чем многие другие типы, но является более сложным и требует дополнительного времени пользователя.

Анализ антропометрических параметров пользователя считается наиболее надежным способом идентификации пользователя, но для его реализации требуется специальное оборудование для удаления и ввода соответствующих параметров и сложных программ для их обработки. Это связано с серьезным удорожанием ИС, что затрудняет широкое использование этого метода. В зависимости от состояния и благополучия человека полученные значения некоторых параметров (например, голоса) будут «плавать», поэтому на практике они полагаются на интегральный подход, когда результат дается для нескольких тестов, принимая во внимание работу с клавиатурой. Каждый человек проявляет свой собственный уникальный почерк клавиатуры. Клавиатурный почерк представляет собой набор динамических характеристик работы на клавиатуре. Многие люди не понимают, что при общении с компьютером личность пользователя проявляется в скорости набора текста, привычке использовать основную или дополнительную часть клавиатуры, природе «двойных» и «встроенных» нажатий клавиш, любимом компьютере методы управления и т.д. Этот метод может быть использован для дополнительной защиты при организации доступа в компьютерных системах. Признание рукописного ввода клавиатуры заключается в выборе соответствующей ссылки из списка стандартов, хранящихся в памяти компьютера, на основе оценки степени близости к этому стандарту параметров рукописного ввода одного из операторов, имеющих право работать с этим компьютером. Решение задачи идентификации пользователя сводится к

решению проблемы распознавания образов[53].

Электронный ключ - это внешнее устройство (обычно для USB, LPT или COM-порт) для идентификации пользователя. Структурно электронные ключи могут быть выполнены в виде электронных карт, электронных планшетов (например, типа iButton), USB-устройств и т.д. Такие ключи подключаются к порту компьютера или работают на одном из каналов беспроводной передачи данных - Wi-Fi, Bluetooth, инфракрасный порт. Электронный ключ обеспечивает приемлемый уровень защиты и, в то же время, обеспечивает наименьшее количество неудобств для конечных пользователей.

Электронные ключи можно классифицировать следующим образом:

- ключи, содержащие только память. Этот класс ключей морально устарел из-за ограниченных возможностей.

- клавиши на ASIC-чипе (ASIC - ApplicationSpecificIntegratedCircuit, применяется специальная интегральная схема). На сегодняшний день это самый распространенный класс ключей, ключи стабильны и надежны в работе. Их функциональность определяется конкретным типом чипа ASIC. Недостатком таких ключей является жесткость конструкции: диапазон их возможностей ограничен кадрами, определяемыми созданием чипа. Все ключи одной и той же модели работают по одному и тому же алгоритму или алгоритмам (т.е. содержат одни и те же функции). Эта функция может отрицательно повлиять на степень стабильности системы защиты.

- микропроцессорные ключи. Этот тип ключей, в отличие от предыдущего, имеет гораздо более гибкое устройство. Контроллер ключа микропроцессора может быть «свернут» программой, которая реализует функции, разные для каждого клиента. В принципе, любой микропроцессорный ключ можно запрограммировать так, чтобы он работал по своему собственному, уникальному алгоритму.

---

[53] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 61.

Дифференциация доступа к элементам защищенной информации.

Под разграничением доступа понимается ограничение возможности использования системных ресурсов по программам, процессам или другим системам (для сети) в соответствии с правилами контроля доступа.

Основным направлением средств контроля доступа являются общие ресурсы. Совместное использование объектов создает ситуацию «взаимного недоверия», при которой разные пользователи одного объекта не могут полностью доверять друг другу. Затем, если что-то происходит с этим объектом, все они попадают в круг подозреваемых.

Существует четыре основных способа совместного доступа к общему объекту:

1) физические субъекты относятся к физически различным объектам (например, устройствам, наборам данных на разных носителях и т.д.);

2) время - субъекты с различными правами доступа к объекту получают его с разными интервалами;

3) логические субъекты получают доступ к общему объекту в пределах одной операционной среды, но под контролем инструментов контроля доступа, которые имитируют виртуальную операционную среду «один объект - все объекты», в этом случае разделение может быть реализовано в различных способы: разделение исходного объекта, разделение с копированием объекта и т.д.;

4) криптографический - все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для дешифрования объекта[54].

Регистрация и анализ событий, происходящих в системе. Механизм регистрации обеспечивает получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрации действий, признанных администрацией IP как потенциально

[54] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 62.

опасных для безопасности системы. Анализ собранной информации позволяет идентифицировать средства и априорную информацию, используемые нарушителем при воздействии на систему и определять, насколько далеко прошло нарушение, предложить метод его расследования и как исправить ситуацию. Таким образом, задачи, которые необходимо выполнить при регистрации и анализе событий, происходящих в системе, выглядят следующим образом:

1) контроль за использованием защищенной информации;

2) выявление попыток несанкционированного доступа к информации;

3) накопление статистических данных о функционировании системы защиты.

3. Защита компьютерной информации от копирования

Рассмотрите задачу защиты компьютерной информации от несанкционированного удаления ее копии. Средства защиты от копирования различаются в определенных функциях, поскольку, с одной стороны, они должны разрешать доступ к законному пользователю, а с другой стороны, запрещать операцию чтения для предотвращения несанкционированного копирования.

Эта задача может быть выполнена следующими способами:

- разрешить операцию чтения (копирования), но сделать копии программы неработоспособными (например, путем «привязки» к аппаратным средствам)

- затруднять чтение информации стандартными средствами, но доступно для специального программного обеспечения,

- создание жестких копий.

Основными функциями, которые система защищает от копирования, являются следующие:

1) идентификация (то есть назначение отдельной трудно идентифицируемой отличительной особенности) этой среды (компьютерного

носителя или персонального компьютера), из которого будет запущена защищенная программа;

2) аутентификация (признание) среды, из которой получен запрос на копирование защищенной программы;

3) регистрация разрешенного копирования;

4) реагирование на попытки несанкционированного копирования;

5) противодействие изучению алгоритмов системы защиты[55].

Подсистемой защиты программы от копирования понимается система, которая обеспечивает ее выполнение своих функций только при распознавании какого-то уникального не скопируемого элемента, называемого ключом. В качестве ключевого элемента могут быть характеристики определенной части компьютерного оборудования (жесткий диск, материнская плата, BIOS) или специальные устройства. Если программный элемент не соответствует аппаратной и программной среде в начале программы, программа завершается.

Для защиты от копирования оптических носителей наиболее распространенными являются:

- запись на предварительно подготовленной среде, поверхность которой содержит ряд неустранимых дефектов, которые не мешают чтению, но которые в корне препятствуют перезаписи диска (степень защиты относительно низкая);

- измените файловую систему, используемую для записи. Этот метод несколько менее универсален, он позволяет защитить данные от возможности незаконного копирования всего диска. Однако усовершенствование дисковых писателей и специального программного обеспечения для копирования защищенных оптических дисков часто позволяет преодолеть защиту, обеспечиваемую двумя первыми методами;

- защищенные диски CD-RX позволяют вам считывать информацию с диска, но вы не можете ее скопировать. На поверхности записи вы можете

[55] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 63.

увидеть небольшой фрагмент данных шириной около 5-6 мм вокруг внутренней окружности диска, на котором записывается VDH - виртуальная цифровая голограмма. «Во время записи записанные данные шифруются и чередуются с использованием уникального диска VDH, поэтому данные могут быть прочитаны только владельцем исходного диска[56].

4. Защита от вредоносного программного обеспечения

Обычно принято ссылаться на вредоносное программное обеспечение или вредоносные закладки, которые копируют, уничтожают, искажают, изменяют информацию и выполняют функции, отключают аппаратное обеспечение, мешают работе компьютера. Есть также такие вкладки, которые только соблюдают, фиксируют все действия, выполняемые законным пользователем, предавая эту информацию злоумышленнику по сети. Компьютерные вирусы, защита которых обсуждается в соответствующем разделе этого руководства, упоминаются как особый вид вредоносной закладки.

Реализация известных в настоящее время закладок возможна с помощью аппаратного или программного обеспечения.

Закладки оборудования могут быть реализованы в процессе изготовления компьютера, ремонта или профилактического обслуживания. Например, ключевой жук может быть замаскирован как адаптер для подключения клавиатуры. Особая опасность аппаратных вкладок заключается в том, что они не могут долго показывать свои вредные эффекты, а затем начинают реализовывать их через определенное время, когда выдается какое-либо событие (например, 31 декабря) или специальная удаленная команда. Раннее обнаружение аппаратных закладок возможно только в условиях специальных проверок с использованием специальных методов и средств.

Программные закладки с точки зрения массового пользователя особенно опасны из-за сравнительной (относительно аппаратной) простоты их

[56] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 64.

реализации, высокой динамичности их распределения и повышенной сложности защиты от них. Таким образом, если в результате специальных проверок аппаратные закладки не были обнаружены или они были устранены (их эффект нейтрализован), то с высокой степенью уверенности в их отсутствии. Закладки программного обеспечения могут появляться в любое время, а ущерб, который они вызывают, не меньше. Например, Keylogger (keylogger, kilogger, keylogger) - программа для отслеживания работы компьютера по функциональности никоим образом не уступает аппаратным устройствам - ошибка клавиатуры.

Основой защиты от вредоносных закладок является следующее:

1) создание условий, при которых дестабилизирующие факторы (ДФ) не могут появиться;

2) предотвращение возникновения ДФ, даже если есть условия для этого;

3) обнаружение появления ДФ;

4) предотвращение воздействия на информацию о возникающих ДФ;

5) выявление негативного воздействия ДФ на информацию;

6) локализация негативного воздействия ДФ на информацию;

7) устранение последствий воздействия ДФ [57].

Таким образом, информация в компьютерных системах может подвергаться случайным или преднамеренным воздействиям. Характер воздействия зависит от конкретных условий работы информационной системы и существующих каналов доступа. При разработке системы безопасности необходимо придерживаться принципов системной, комплексной, непрерывной защиты, разумной достаточности, гибкости управления, открытости алгоритмов и простоты применения защитных мер. Среди существующих мер по обеспечению безопасности информации наиболее эффективными являются физические и технические, выполняющие такие основные функции, как:

[57] Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015. – С. 65.

идентификация, аутентификация и авторизация пользователей, контроль и разграничение доступа к ресурсам, регистрация и анализ событий, мониторинг целостности системных ресурсов. Существуют программные и аппаратные системы, обеспечивающие их реализацию.

Среди всего спектра методов защиты данных от нежелательного доступа криптографические методы занимают особое место. В отличие от других методов, они полагаются только на свойства самой информации и не используют свойства своих материальных носителей, особенности ее узлов обработки, передачи и хранения.

Широкое использование компьютерных технологий и постоянное увеличение объема информационных потоков вызывают постоянный рост интереса к криптографии. В последнее время роль программного обеспечения для защиты информации растет, просто обновляется, что не требует больших финансовых затрат по сравнению с аппаратными криптосистемами. Современные методы шифрования гарантируют почти абсолютную защиту данных.

2.4. Оперативно-розыскная информация и угрозы информационной безопасности в процессе оперативно-розыскной деятельности

Оперативно-розыскная деятельность как множество коммуникативных процессов генерирует оперативно-поисковый информационный процесс (далее - ОРИП), который является единством процессов обработки данных, связанных с операционными поисковыми записями; функционирование оперативно-поисковых записей; формирование базы данных оперативно-розыскных целей. Терминологический состав и структура этой концепции позволяют нам

рассматривать ОРИП с позиции автоматизированной системы, состоящей из сотрудников, и набора средств автоматизации для его деятельности, реализующих информационные технологии для выполнения установленных функций. Специфика оперативно-розыскной деятельности и генерируемой им информации оперативного поиска требует защиты.

Основываясь на понятии информационной безопасности при формулировке профессора А. И. Алексанцева, понятие информационной безопасности подразделений уголовного расследования может быть сформулировано как совокупность следующих трех основных компонентов: 1) состояние информационной среды, обеспечивающее удовлетворение потребности подразделений уголовного расследования в необходимой информации; 2) безопасность информации и телекоммуникаций в распоряжении подразделений уголовного преследования; 3) безопасность сотрудников уголовного преследования и доверенных лиц от негативной информации и психологических последствий[58].

Несмотря на значительную степень законодательного, исследовательского и инженерно-технического изучения проблемы, считается, что проблемы технической защиты не решены полностью, по сравнению с тем, что можно рассмотреть проблемы защиты сотрудников от деструктивной информации и психологических влияний не только плохо работали, но, скорее, как не решаются на данный момент.

Техническая защита информации не является исчерпывающим средством, обеспечивающим необходимый уровень безопасности автоматизированной системы. Использование дорогостоящих технических решений создает иллюзию абсолютной безопасности, а тот факт, что любая система безопасности (техническая, организационная, технологическая) не может функционировать автономно без участия человека - ускользает от нас.

[58] Алексенцев А.И. Конфиденциальное делопроизводство. - ООО «Журнал «Управление персоналом», 2003. – С. 13.

Исследования информационной безопасности автоматизированных систем показывают, что самым слабым элементом является человек или человеческий фактор; со ссылкой на ORIP - сотрудник уголовного розыска, руководитель. Существуют ли объективные причины для этого обстоятельства? Изучение этого вопроса позволяет положительно ответить на вопрос в следующих случаях:

- являясь участником процесса информации и коммуникации, разнообразным из которых является процесс оперативной и поисковой информации, лицо подвержено влиянию внешних факторов, которые влияют на соблюдение правил и правил информационного процесса. В то же время как сами факторы, так и индуцированные поведенческие реакции носят вероятностный характер и, как правило, плохо предсказуемы;

- у оперативного сотрудника, у главы есть свои недостатки. Манипулирование слабостями часто создает возможность контролировать поведение, чтобы изменить технологический процесс обработки информации;

- стремление быть в центре внимания других, заставляет участников ОРИП выполнять необоснованные, а не рациональные действия как в информационных процессах, так и в окружающем информационном пространстве;

- логика реализации кибернетического вычислительного процесса и логика действий в деятельности человека различны. Человек не является машиной, программа его действий не идентична программе вычислительного процесса; он переменный, многофакторный и многогранный; поэтому сложность защиты логики действий человека эквивалентна сложности построения человеческих алгоритмов мышления[59].

Сотрудники уголовного розыска являются неотъемлемой частью ОРИП с присущим им «человеческим фактором», который создает предпосылки и

[59] Косарева Т.В., Федоткин А.И. Способы выявления, предупреждения, пресечения и раскрытия преступлений сотрудниками уголовного розыска в сети Интернет: методические рекомендации. – Домодедово: ВИПК МВД России, 2014. – С. 99.

возможности использования прикладных методов социальной науки, направленных на изменение поведения и отношения сотрудников с целью побудить их к несанкционированному предоставлению защищенных данные. В соответствии с существующей терминологией этот метод называется социальной инженерией. Социальная инженерия - это метод управления человеческими действиями без использования технических средств, он основан на использовании слабых сторон человеческого фактора и считается очень разрушительным.

Для несанкционированного доступа к защищенной информации в дополнение к кибератакам могут использоваться методы социальной инженерии. Разница заключается в том, что в первом случае в качестве объекта нападения используются технические средства, а во втором - психика субъектов инициирующих ОРИП - оперативного персонала, руководителей. Множество способов влияния на социальную инженерию очень разнообразно. Однако из-за уникальности нравственных, моральных, умышленных установок каждого человека, особенностей социального статуса, гражданской позиции и отношения к выполнению своих обязанностей нет универсальных решений для несанкционированного доступа к защищенной оперативно-поисковой информации в социальных машиностроение.

По мнению экспертов, наиболее часто используемыми и эффективными являются следующие методы: непосредственное воздействие; обратный инжиниринг; сбор и исследование информации из открытых источников, вводящей в заблуждение. Для практики ОРИП эти методы могут быть двух видов. С одной стороны, это особый арсенал оперативного сотрудника, используемого для информационной конфронтации в процессе ОРИП. С другой стороны, - как угроза деструктивного информационного воздействия на субъектов - участников ОРИП.

Наиболее эффективными методами социальной инженерии являются:

- метод прямого удара. Целью метода является получение защищенной

оперативно-поисковой информации. Поскольку объектом атаки являются оперативные сотрудники, задействованные в технологии обработки поступающего и исходящего потока документов высокой интенсивности. Особые навыки атакующего человека - овладение терминологией и суть проблем, связанных с действиями атакованных. Основой метода является состояние доверия, взаимопомощи, желание помочь. Тактикой атаки является введение атакованного оперативного офицера в срочное решение. Пример реализации атаки: злоумышленник называет участника ОРИП и формирует определенный коммуникативный процесс. Во время постановки вопроса злоумышленник вводит атакующего оперативного сотрудника в срочный режим принятия решений. Например, он сообщает, что он выполняет срочную и важную работу, для эффективной реализации которой требуется срочно прояснить некоторые данные. После слов «требуется уточнить», злоумышленник сообщает о предмете его интереса. Эта тактика провоцирует атакующего сотрудника на отказ от правил обращения с защищенной информацией, что создает вероятность утечки данных, которая необходима злоумышленнику. Краткая продолжительность атаки и интенсивность процесса обслуживания атакующего определяют, что атакующий офицер без помощи со стороны не вспоминает человека, который подал заявление, и переданную ему информацию;

- метод обратной инженерии. Целью метода является получение защищенной оперативно-поисковой информации. В качестве объектов атаки участвуют участники ОРИП. Особые навыки атакующего - это возможность войти в доверие. Нападающий должен знать о личной жизни, увлечениях, слабостях, моральных и моральных особенностях поведения, убеждениях и стереотипах атакованного оперативного сотрудника. Основой метода является необходимость нападающего в дружественной обстановке, дружбе, состоянии доверительных отношений. Особенностью метода является его значительная продолжительность. Чувство комфорта, созданное неформальной атмосферой,

профессиональное скучное чувство бдительности и конфиденциальной атмосферы, вызывает возможность раскрытия защищенной информации, которая стала известна оперативному сотруднику в ходе официальных обязанностей[60].

В качестве примера комбинированных методов социальной инженерии и современных информационных технологий можно привести:

- метод введения в заблуждение (фишинг), основанный на характеристиках человека, которому доверяют давно используемые вещи, объекты, ресурсы; создание на их основе суррогатов для получения необходимой информации (английский промысел - рыбалка, рыбалка);

- метод сбора и исследования информации из открытых источников. Эффективность этого метода определяется техно-социальным феноменом XXI века. Название социальных сетей активно использует человеческие библейские пороки - суету, гордость и зависть. Стремление к саморекламе, похваляющееся вызывает неконтролируемую самопубликуемую публикацию в социальной сети личной информации, касающейся официальных событий и личной жизни. Информация, опубликованная в социальной сети, становится общедоступной.

Информационные атаки с использованием методов социальной инженерии создают угрозу информационной безопасности подразделений уголовного розыска. Противодействие методам социальной инженерии может быть организовано с использованием, прежде всего, организационных и регуляторных мер, которые гласят:

- изучение кандидата при подаче заявления на работу, в том числе путем проведения проверочных мероприятий, направленных на всестороннее изучение его личных качеств, окружающей среды, областей интересов, биографии работы;

- проведение занятий с сотрудниками Департамента уголовного розыска в

[60] Косарева Т.В., Федоткин А.И. Способы выявления, предупреждения, пресечения и раскрытия преступлений сотрудниками уголовного розыска в сети Интернет: методические рекомендации. – Домодедово: ВИПК МВД России, 2014. – С. 100.

соответствии с правилами работы с безопасной оперативной информацией и обучения навыкам противодействия методам социальной инженерии;

- контроль соблюдения технологии обработки информации;

- образовательная работа, связанная с повышением мотивации и бдительности сотрудников;

- мониторинг профессиональной пригодности сотрудников с точки зрения обеспечения информационной безопасности (возможно, с использованием технических инструментов для инструментальных психофизиологических исследований);

- организация контроля за появлением официальной информации и другой конфиденциальной информации в открытых источниках информации.

В качестве дополнительных мер вы можете использовать:

- контроль входящей электронной корреспонденции, поступающей в почтовые ящики сотрудников, независимо от уровня официальной позиции;

- контроль содержания официальных телефонных разговоров сотрудников с использованием официальных средств связи.

Обеспечение деятельности сотрудников в рамках утвержденных правил является одной из задач управленческой команды. Осознание проблем, выявленных руководством и каждым сотрудником по уголовным расследованиям, является эффективной превентивной мерой по минимизации рисков от угроз несанкционированного доступа к оперативной и поисковой информации с использованием методов социальной инженерии.

ЗАКЛЮЧЕНИЕ

В заключение выпускной квалификационной работы можно сделать следующие выводы.

В современных условиях информационная безопасность общества, государства и личности наряду с другими видами безопасности, в том числе экономическими, является важнейшим компонентом национальной безопасности.

Угрозы информационной безопасности страны, источниками которой являются современные национальные и транснациональные преступные сообщества, которые охватывают все их масштабы и масштабы в масштабах всей страны и затрагивают все сферы общества, подрывают национальную безопасность Российской Федерации, вызывая это значительный урон.

Органы внутренних дел МВД России являются важной составляющей сил и средств противодействия посягательствам на информацию преступных сообществ на права и свободы граждан, безопасность государства, общества и личности.

Как показывает практика правоохранительных органов последних лет, вышеупомянутые формулировки не в полной мере обеспечивают защиту официальных секретов в деятельности правоохранительных органов. Эта ситуация, на наш взгляд, объясняется тем, что в нормах действующего уголовного законодательства нет систематического подхода к формированию защиты служебных секретов. Предоставление этим категориям информации статуса официальных секретов и введение отдельной статьи для ее раскрытия и других незаконных действий позволило бы исключить из Уголовного кодекса Российской Федерации во многих отношениях совпадающие композиции и определить ответственность. Для достижения этой цели, основанной на анализе вышеупомянутых преступлений, мы предлагаем наше концептуальное видение решения проблемы комплексной защиты служебных секретов, когда

правоохранительные органы выступают в качестве одного из участников уголовного права связи.

Защита служебных секретов в деятельности органов внутренних дел нормами уголовного права должна рассматриваться в следующих аспектах:

- когда сами сотрудники ОВД действуют как субъекты преступления в связи с совершением противоправного деяния с информацией, которая содержит официальную тайну, полученную при осуществлении официальных полномочий;

- когда должностные лица ОВД обязаны принимать законные меры для пресечения незаконной деятельности с информацией, содержащей официальную тайну, полученную лицом, имеющим доступ к нему на законных основаниях. Рассмотрение этих аспектов проблемы должно проводиться взаимосвязанным образом, поскольку именно этот порядок позволяет в комплексе обеспечить уголовную и правовую защиту служебных секретов в органах внутренних дел. Существование в Уголовном кодексе языка, направленное на защиту служебных секретов, не позволяет нам сегодня говорить о какой-либо полноте, они не полностью отражают реальное положение вещей в этой области.

Исходя из вышесказанного, мы считаем, что способность эффективно решать проблемы безопасности информации, составляющей государственную тайну в органах внутренних дел, будет во многом зависеть от формирования единой службы, которая будет отвечать за весь комплекс мер по защите информации в своей деятельности.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Окинавская хартия Глобального информационного общества. Принята главами государств и правительств «Группы восьми» 22 июля 2000 года // Дипломатический вестник. – № 8. – 2000.– С. 51-56.
2. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с изм. от 21 марта 2014 г. N 6-ФКЗ) // Российская газета от 25 декабря 1993 г. N 237; Собрание законодательства Российской Федерации. - 2014. - N 31. - ст. 4398.
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (с изм. от 31.12.2017 г. №499-ФЗ) // Российская газета от 31 декабря 2001 г. №256; Справочно-правовая система Гарант.
4. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изм. от 19 февраля 2018 г. №25-ФЗ) // Собрание законодательства Российской Федерации. – 1996. - №25. – Ст. 2954; Справочно-правовая система Гарант.
5. Федерального закона Российской Федерации от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации» (31 декабря 2017 г.) // СЗ РФ. – 2006. - №31 (Часть I). – Ст. 3448; Справочно-правовая система Гарант.
6. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (с изм. от 26.07.2017 № 193-ФЗ) // Российская газета. – 21 сентября 1993. - №182; от 31 июля 2017 г. №167.
7. Федерального закона Российской Федерации от 27.07.2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации» (31 декабря 2017 г.) // СЗ РФ. – 2006. - №31 (Часть I). – Ст. 3448; Справочно-правовая система Гарант.
8. Федеральный закон Российской Федерации от 03.04.1995 г. № 40-ФЗ «О

Федеральной службе безопасности» (с изм. от 18 июня 2017 г. №127-ФЗ) // СЗ РФ. – 2017. - №25. – Ст. 3596.

9. Федеральный закон Российской Федерации от 03.04.1995 г. № 40-ФЗ «О Федеральной службе безопасности» (с изм. от 18 июня 2017 г. №127-ФЗ) // СЗ РФ. – 2017. - №25. – Ст. 3596.

10. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. – 2016. - №1 (Часть II). – Ст. 212.

11. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” // Собрание законодательства Российской Федерации. – 2016. - №50. – Ст. 7074.

12. Постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011-2020 годы)» (с изм. от 15 ноября 2017 г. №1384). // СЗ РФ. – 2017. - №47. – Ст. 7007.

13. Распоряжение Правительства Российской Федерации № 1701-р от 22.10.1999 г. «Об усилении борьбы с преступлениями в сфере высоких технологий и реализации международных договоренностей и обязательств Российской Федерации» // СЗ РФ. – 1999. - №44. – Ст. 5335.

Материалы судебной практики

14. Официальный сайт Чертановского районного суда г. Москвы. Решение по уголовному делу № 1-618/2013 в отношении И.О. Сюриса [Электронный ресурс]. – Режим доступа: https//www.chertanovsky--msk.sudrf.ru/modules.php?name=sud_delo&name_op=doc&srv_num=1&number=212030021&delo_id=1540006&new=&text_number=1.

15. Официальный сайт Хорошевского районного суда г. Москвы. Решение по уголовному делу № 1-667/2014 в отношении С.С. Ларина [Электронный ресурс]. – Режим доступа: https://www.horoshevsky—

msk.sudrf.ru/modules.php?name=sud_delo&name_op=doc&srv_num=1&number=223994530&delo_id=1540006&new=&text_number=1.

Специальная литература

16. Алексенцев А.И. Конфиденциальное делопроизводство. - ООО «Журнал «Управление персоналом», 2003.

17. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е.Основы информационной безопасности. Учебное пособие. - Иркутск, ФГОУ ВПО ВСИ МВД России, 2015.

18. Богланова Т.Н. Вестник Челябинского государственного университета. – 2012. – № 37 (291). Право. – Вып. 34.

19. Вортоников В.Л. Актуальные вопросы квалификации преступлений в сфере компьютерной информации. // Вестник ТГУ. – 2009. – Вып. 5 (73).

20. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления. // Бизнес-информатика. – 2013. – № 2 (24).

21. Зейналов, Г.Г. Глобализация как фактор современного развития / Г.Г.Зейналов, О.И. Немыкина // Учебный эксперимент в образовании. 2011. № 2. С. 4.

22. Карамнов А.Ю. Уголовная ответственность за неправомерный доступ к компьютерной информации: проблемы теории и правоприменительной практики. // Право и общество. – 2010. – № 6 (022).

23. Козориз Н. Л. Информационная безопасность в системе противодействия опасности // Информационное право. – 2013. – № 1. – С. 30.

24. Количество пользователей интернета в России // Интернет в России и в мире [Электронный ресурс]. - Режим доступа: http://www.bizhit.ru/ index/users_count/0-151.

25. Комментарий к Ст. 272 УК РФ // Уголовный Кодекс Российской Федерации со всеми изменениями и дополнениями. Комментарий к статьям УК РФ [Электронный ресурс]. - Режим доступа: http://stykrf.ru/272.

26. Кондратов М.А. К постановке вопроса об уголовной ответственности юридических лиц в уголовном праве России (исторический аспект) / М.А. Кондратов, С.С. Медведев // Научный журнал КубГАУ - Scientific Journal of KubSAU. - 2015. - №106 [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/article/n/k-postanovke-voprosa-ob-ugolovnoy-otvetstvennosti-yuridicheskih-lits-v-ugolovnom-prave-rossii-istoricheskiy-aspekt.

27. Косарева Т.В., Федоткин А.И. Способы выявления, предупреждения, пресечения и раскрытия преступлений сотрудниками уголовного розыска в сети Интернет: методические рекомендации. – Домодедово: ВИПК МВД России, 2014.

28. Кутахов, Ю.Л. Человек. Полиэтнический мир. Безопасность / Ю.Л. Кутахов , Р. А. Явчуновская. СПб., 1998. 404 с.

29. Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ - Scientific Journal of KubSAU. - 2013. - №90 [Электронный ресурс]. - Режим доступа: http://cyberleninka.ru/ article/n/problemy-kvalifikatsii-prestupleniy-v-sfere-kompyuternoy-informatsii-1.

30. Медведев С.С. Мошенничество в сфере высоких технологий: Дис. ... канд. юрид. наук: 12.00.08 / Медведев Сергей Сергеевич; Кубан. гос. аграр. ун-т. - Краснодар, 2008. – С. 24.

31. Нагорный А.А. Проблемы квалификации преступлений в сфере компьютерной информации // Oaji.net [Электронный ресурс]. - Режим доступа: http://oaji.net/articles/2014/245-1393744181.pdf.

32. Немыкина О. И. Теоретический анализ проблем информационной безопасности современного общества Теория и практика общественного развития. 2011. № 1. С. 43-44.

33. Основы информационной безопасности органов внутренних дел : учебное пособие / В.А. Кемпф. – Барнаул : Барнаульский юридический институт МВД России, 2014.

34. Пасхин, Е.Н. Устойчивое развитие и информатизация образования / Е.Н. Пасхин, В.Г. Тупало, А.Д. Урсул. М.: Изд-во РАГС. 2007.

35. Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. матер. всерос. науч.-практ. конф., Воронеж, 16-17 апреля 2015 г. / под ред. д-ра юрид. наук А.Л. Осипенко. – Воронеж: Воронежский институт МВД России, 2015. – 139 с.

36. Терещенко Л. К Модернизация информационных отношений и информационного законодательства: Монография. – М. : ИНФРА-М. – 2013. – С. 158.

37. Холопова Е. Н., Бойцов А. С. Информационная безопасность пограничных органов на современном этапе: понятие, структура // Информационное право. – 2014. – № 5. – С. 6.

38. Швецов А.В. Административно-правовое регулирование служебной тайны / А.В. Швецов, Т.М. Занина II IV Всероссийская научно-практическая конференция «Охрана, безопасность и связь»: Сборник материалов. Часть 2. - Воронеж: Воронежский институт МВД России, 2013. – С. 77.

39. Швецов А.В. Свойства и признаки, отличающие служебную тайну от других видов тайн / А.В. Швецов // Вестник Воронежского института МВД России. - Воронеж: ВИ МВД России. -№. 5 (24). 2005.

40. Швецов А.В. Формирование института служебной тайны на современном этапе / А.В. Швецов, Т.М. Занина И Всероссийская научно-практическая конференция «Государство, право, общество: современное состояние и проблемы развития». - Липецк: Липецкий филиал Воронежского института МВД России, 2013. – С. 56.

РЕЦЕНЗИЯ
на выпускную квалификационную работу

слушателя Яруллина Рузеля Маратовича
(фамилия, имя, отчество)
131 учебная группа, 5 курс, специальность – правовое обеспечение
(№ группы, курс, специальность, факультет)
национальной безопасности

Тема: Обеспечение информационной безопасности в ОВД

Представленная для рецензирования выпускная квалификационная работа посвящена исследованию вопросов, касающихся информационной безопасности в органах внутренних дел Российской Федерации. Выбранная тема является весьма актуальной, поскольку на сегодняшний день в органах внутренних дел уделяется особое внимание вопросам сохранения секретных сведений, воспитанию у сотрудников высокой бдительности. Однако некоторыми из них часто недооценивается опасность утечки информации ограниченного доступа. В работе автором точно сформулированы цели и задачи, которые соответствуют названию работы.

Работа структурно состоит из введения, двух глав, включающих семь параграфов, заключения и списка использованной литературы. Структура выпускной квалификационной работы соответствует указанным целям и задачам. Содержание соответствует названию параграфов, части работы соразмерны.

Автор осветил вопросы темы выпускной квалификационной работы на высоком научном уровне в полном объеме. Во введении автором определена актуальность темы исследования, объект и предмет научного исследования, цель, задачи, теоретическая и практическая значимость. В первой главе исследования раскрывается общая характеристика информационной безопасности и её нормативно-правовое регулирование. Вторая глава

посвящена организационным основам информационной безопасности в органах внутренних дел Российской Федерации. При написании ВКР автором использованы основные методологические и теоретические подходы к решению проблемы, изучены основные теоретические работы, посвящённые проблеме выпускной квалификационной работы, проанализированы научные взгляды, проведен сравнительно-сопоставительный анализ источников. Выводы и предложения, выдвинутые автором в заключении, обоснованны и аргументированы. Прослеживается высокая степень самостоятельности автора при раскрытии вопросов темы и решении поставленной задачи. Имеются обоснованные теоретические выводы и предложения по совершенствованию законодательства России.

Яруллин Р.М. показал знание нормативно-правовых актов, профессиональной литературы, источников, фундаментальных исследований по теме, публикаций ведущих специалистов в области темы исследования. В списке использованной литературы приведено достаточное количество законов Российской Федерации и иных нормативных актов, указаны авторефераты диссертаций по указанной тематике, а также научные статьи и электронные источники.

В заключении автор обобщил выводы по каждой главе, предложил варианты решения поставленных задач и обосновал выбранные методы. Выводы соответствуют целям, задачам и методам работы, логичны и обоснованны.

Существенных недостатков в ВКР не выявлено.

При написании ВКР автор показал высокий уровень грамотности, научный стиль изложения. Работа и отдельные элементы текста оформлены в соответствии с предъявляемыми требованиями, уровни заголовков и подзаголовков соблюдены, имеются ссылки на нормативно-правовые акты, работы и источники, указанные в списке литературы. В целом работа выполнена аккуратно.

Представленная на рецензирование выпускная квалификационная работа «Обеспечение информационной безопасности в органах внутренних дел Российской Федерации» соответствует предъявляемым требованиям, рекомендована к публичной защите и заслуживает оценки «отлично».

Оценка рецензента отлично

Рецензент

Начальник ОД ОМВД России
по Альметьевскому району
подполковник полиции Г.М.Смоленкова

М.П.

«7» мая 2018 г.

Отзыв

о ходе выполнения выпускной квалификационной работы слушателя 131 учебной группы Яруллина Рузеля Маратовича

на тему: «Обеспечение информационной безопасности в органах внутренних дел Российской Федерации»,

Данная тема выпускной квалификационной работы является весьма актуальной в связи с тем, что обеспечение информационной безопасности является одной из наиболее острых проблем не ТОЛЬКО ДЛЯ РОССИИ, НО И во всем мировом пространстве.

Обеспечение информационной безопасности осуществляется с применением технических и организационных мер в соответствии с требованиями нормативных правовых актов РОССИЙСКОЙ Федерации И нормативных правовых актов МВД России, регламентирующих данную сферу деятельности. Все выше указанное позволяет призвать

целесообразным структуру выпускной квалификационной работы:

К положительным сторонам выпускной квалификационной работы следует отнести комплексный анализ решения проблемы обеспечения информационной безопасности, требующей для своего совместных усилий министерств, ведомств, других государственных органов, многих предприятий и организации, что корректно сформулировано в целях и задачах своей исследовательской деятельности При выполнении выпускной квалификационной работы.

За время исследовательской работы Яруллин Р.М, проявил себя как старательный слушатель, постоянно повышал свой профессиональный уровень,

использовал и умело обобщал эмпирический материал по тематике выпускной квалификационной работы,

Данная работа содержит некоторые недостатки, например небольшой объем статистических данных последних лет, которые можно (было бы представить для наглядности схематически или графически. Данные недостатки являются несущественными и не влияют на общую оценку выпускной квалификационной работы.

Яруллин Р.М. продемонстрировал хорошие аналитические способности, умение анализировать и систематизировать собранную информацию, а также делать самостоятельные выводы, предложения и обобщения.

Выпускная квалификационная работа слушателя выполнена в соответствии с рекомендациями и требованиями по оформлению выпускных квалификационных работ вузов. В работе есть логичность изложения анализа, изложенный текст в исследовании ПОЛНОСТЬЮ соответствует названиям разделов, присутствовала пунктуальность в выполнении структурных элементов работы в установленные научным руководителем сроки.

При выполнении выпускной квалификационной работы слушатель грамотно и аргументировано выбрал программные средства и технологии, необходимые для решения поставленных в работе задач 6 учетом современных требований и подходов к обеспечению информационной безопасности.

В достаточной степени использованы теоретические и нормативные источники по теме выпускной квалификационной работы,

Выпускная квалификационная работа должна быть допущена к защите с высокой положительной оценкой.

Кандидат педагогических наук
доцент кафедры экономики, финансового права
и информационных технологий в ОВД
подполковник полиции

ММ

Е,Э* Турутина

Подпись

УДОСТОВЕРЯЕТСЯ
ОД н Р КЮИ МВД Росени

АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

УВАЖАЕМЫЙ ПОЛЬЗОВАТЕЛЬ!

Обращаем ваше внимание, что система «Антиплагиат» отвечает на вопрос, является ли тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение. Данный отчет не подлежит использованию в коммерческих целях.

Отчет о проверке на заимствования №1

Автор: Шевко Наиля Рашидовна nailya-shevko@rambler.ru / ID: 57
Проверяющий: Шевко Наиля Рашидовна (nailya-shevko@rambler.ru / ID: 57)
Организация: Казанский юридический институт МВД России

Отчет предоставлен сервисом «Антиплагиат» - http://кюи.ап.мвд.рф

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 9
Начало загрузки: 03.07.2018 13:08:03
Длительность загрузки: 00:02:08
Имя исходного файла: Дипломная работа Яруллин Р.М.
Размер текста: 376 кБ
Символов в тексте: 126440
Слов в тексте: 14503
Число предложений: 804

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 03.07.2018 13:10:11
Длительность проверки: 00:00:09
Комментарии: не указано
Модули поиска: Модуль поиска ЭБС "БиблиоРоссика", Модуль поиска ЭБС "BOOK.ru", Коллекция РГБ, Цитирование, Модуль поиска ЭБС "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Коллекция ГАРАНТ, Модуль поиска ЭБС "Айбукс", Модуль поиска Интернет, Модуль поиска "КЮИ МВД РФ", Модуль поиска ЭБС "Лань", Сводная коллекция вузов МВД, Кольцо вузов

ЗАИМСТВОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
39,92%	7,54%	52,54%