Краснодарский университет МВД России

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ПРИ РАБОТЕ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Учебное пособие

Краснодар
2023

УДК 004.056.5(075.8)
ББК 16.8
О-931

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *М. А. Ледовская, К. Н. Богданова*

Рецензенты:
А. И. Локнов, кандидат технических наук (Санкт-Петербургский университет МВД россии);
В. Г. Якименко (Главное управление МВД России по Краснодарскому краю).

Оценка информационных рисков при работе со служебной
О-931 информацией ограниченного распространения : учебное пособие / сост.: М. А. Ледовская, К. Н. Богданова. – Краснодар : Краснодарский университет МВД России, 2023. – 76 с.

ISBN 978-5-9266-1918-5

Содержатся теоретические аспекты работы со служебной информацией ограниченного распространения, анализируются методы повышения эффективности обеспечения информационной безопасности при работе со служебной информацией ограниченного распространения, подходы к оценке рисков информационной безопасности.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 004.056.5(075.8)
ББК 16.8

ISBN 978-5-9266-1918-5

© Краснодарский университет
МВД России, 2023
© Ледовская М. А., Богданова К. Н.,
составление, 2023

Введение

Актуальность работы обусловлена показателями сложившейся мировой ситуации, когда страны движутся по пути перехода от индустриального общества к информационному, где материальные и энергетические ресурсы уступают информационным. Под информационными ресурсами принято понимать отдельные документы и массивы документов в информационных системах (библиотеки, архивы, банки данных, и другие). Информационные ресурсы – собственность, находящееся в ведении соответствующих органов и организаций, подлежащая учету и защите. В современных представлениях информация может быть использована в качестве товара, превращена в деньги. Она является ценным ресурсом, на который компании и организации расходуют крупные средства, с целью максимальной защиты информации от утечки и кражи.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах информационного взаимодействия.

Это и сформировало наш интерес к данной проблеме и определило цель исследования, которое заключается в изучении и организации оценки информационных рисков при работе со служебной информацией ограниченного распространения.

Реализация поставленной цели потребовало постановки и последовательного решения следующих задач:

1. Изучить понятие, виды и сферы применения служебной информации ограниченного распространения.

2. Рассмотреть классификацию информационных рисков при работе со служебной информации ограниченного распространения.

3. Проанализировать воздействия на процесс обработки служебной информации ограниченного распространения.

4. Изучить угрозы информационных рисков служебной информации ограниченного распространения в системе Министерства внутренних дел Российской Федерации.

5. Произвести исследование подходов к анализу оценки информационных рисков.

6. Организовать методику оценивания информационных рисков со служебной информации ограниченного распространения.

Необходимость достижения поставленной цели определила объект и предмет данного исследования.

Объектом исследования является законодательство Российской Федерации в сфере работы со служебной информации ограниченного распространения.

Предметом исследования выступает организация оценки информационных ресурсов при работе со служебной информации ограниченного распространения.

Степень разработанности проблемы. Вопросы исследования уровня защиты служебной информации ограниченного распространения достаточно широко распространяются учеными. Значительный вклад в теорию и методику анализа защиты служебной тайны внесли такие ученые как А.А. Грушо, Е.Е. Тимонина, П.Н. Кораблев, Т.М. Занина, П.Д. Зегжда, С.П. Расторгуев.

Авторами широко освещается проблемы развития как информационной безопасности в целом, так и отдельных ее компонентов.

Теоретическая и практическая значимость учебного пособия заключается в том, что минимизация негативного влияния на служебную информацию ограниченного распространения позволит обеспечить стабильное функционирование и использование информационных ресурсов между участниками организованной деятельности.

Проведенный в исследовании анализ уровня информационных ресурсов при работе со служебной информации ограниченного распространения согласно действующим методикам, является основой для разработки и реализации мероприятий по повышению уровня информационной безопасности, имеющих практическую направленность для каждого подразделения.

Теоретической и методической базой исследования явились нормативные правовые акты Российской Федерации, учебно-методическая и учебно-практическая литература, публикации в изданиях для специалистов по защите информации. Эмпирической базой выполнения работы послужила деятельность отдела делопроизводства и режима секретности.

В работе были использованы как общенаучные, так и частные научные методы исследования: анализ, синтез, системный, формально-логический, структурно-функциональный, историко-правовой, сравнительно-правовой методы. Указанные методы применялись в сочетании с требованиями объективности, всесторонности и принципа конкретности познания.

Структура работы определена целью и решаемыми задачами исследования и состоит из введения, трех глав, заключения и списка использованных источников.

1. Теоретические аспекты оценивания информационных рисков при работе со служебной информацией ограниченного распространения

1.1. Понятие, виды и сфера применения служебной информации ограниченного распространения

Работа человека с информацией берет свое начало со времен древних государств, когда люди начали понимать значение и важность получаемых сведений, а также их нежелательное распространение. Аппарат государственного управления считал одной из своих главных задач – охрану государственных секретов. Одной из самых древних и по настоящее время значимых тайн можно назвать военную тайну, которая подразумевает под собой ограничение доступа к информации военно-промышленного характера, о стратегии и тактики ведения боя, местах дислокации подразделений и воинских частей.

Начиная с давних времен, отношения между правителем и подчиненными регулировались в форме присяги, однако акцент на сохранение в тайне государственных дел поставлен не был. Службу следовало нести «без хитрости». Однако с 1653 года была утверждена новая форма присяги, где чиновникам некоторых должностей предписывалось ограничение на распространение информации, полученной в ходе своей деятельности, «до Государева указа». Происходит становление тенденции постепенного засекречивания государственных дел и государственной службы.

Упоминание о секретах в сфере государственного управления встречается в Генеральном регламенте 1720 года. Однако, к этому времени понятие «тайна государственного управления» сформулировано не было, как и самих критериев и порядка отнесения информации к тайной. Несмотря на это, в нормативном правовом акте прописаны три наиболее важных аспекта правового регулирования:

1. Обязанность государственных служащих хранить тайну (процедура «допуска» к тайне в форме клятвы);
2. Необходимость ведения дел тайно;
3. Предусмотрено наказание за разглашение тайны.

В Петровскую эпоху появляется секрет (тайна) государственной службы. Деления информации по видам тайн еще не было, однако стали разрабатываться основные положения, регулирующие порядок допуска, сохранность, обращение с информацией такого рода, а также наказание, связанные с разглашением тайны, которые были прописаны в законодательстве.

Эпоха Екатерины II ознаменовано появление пометок «секретно» на документах и конвертах. С целью совершенствования делопроизводства был создан Сенатский приказ в 1768 году, в котором особе внимание уделялось нарушением действующего порядка обращения с секретными документами. Определялись конкретные лица, уполномоченные на подписание секретных документов. Приказом устанавливался конкретный штраф, в размере 10 рублей, за нарушение предписанного порядка обращения с такими документами.

В начале XX века в связи с внешне- и внутриполитическими процессами, охрана государственных секретов стала приобретать широкие масштабы. В них входили как защита государственной тайны, так и борьба со шпионажем. В учебнике под редакцией академика Б.Н. Топорнина «Информационное право» [1] пишется о наличие в Советском Союзе трех видов информации ограниченного доступа: государственная тайна (документы с грифами «Особой важности», «Совершенно секретно»), служебной тайны («секретно») и документы «Для служебного пользования». В 20-х гг. XX века советское государство делило информацию на 2 вида:

1. Специально охраняемая тайна (в нынешнее время она же «государственная тайна»);
2. Сведения, не подлежащие оглашению (при этом не составляли охраняемую государственную тайну). Однако данные сведения защищались уголовно-правовыми и иными средствами наряду с государственной тайной.

Содержание служебных сведений, не подлежащих оглашению и входивших в состав служебной тайны, составляли разнообразные сведения, в том числе отражавшие текущую управленческую деятельность государственных структур и ее результаты, распространение которых могло повлиять на эффективность данной деятельности. Выделялось два вида таких сведений: ограничение доступа к которым диктовалось объективными потребностями государственного

управления, и сведения, разглашения которых могло повлиять на политическую обстановку среди гражданского населения.

Различие грифов и пометок устанавливалось исходя из уровня ущерба для государственной безопасности, а также в связи с необходимостью сохранения авторитета государства и его структур.

Рис.1. Виды информации по способу распространения

В настоящее время, в соответствии со статьей 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, информация разграничивается по способу распространения – ограниченного доступа и общедоступная. Сведения ограниченного распространения – это данные, которые используются с согласия (разрешения) их владельца. Общедоступная информация, в свою очередь, подразумевает сведения, которые не защищаются законодательно.

Деятельность органов внутренних дел в значительной мере связана с получением и использованием информации ограниченного доступа, разглашение которой может спровоцировать нарушение конституционных прав граждан и снижение эффективности службы правоохранительных органов по предупреждению, пресечению и раскрытию преступлений.

В соответствии с постановлением Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обра-

щения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе по космической деятельности» к служебной информации ограниченного распространения относится:

1. Несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуется служебной необходимостью.

2. Поступившая в организацию несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.

Разграничение информации, циркулирующей в органах внутренних дел, можно представить в виде:

1. Образовавшееся в ходе оперативно служебной деятельности (информация внутри системы).

2. Поступившая из внешней среды (из сторонних организаций, от граждан, органов исполнительной власти и др.).

К первому виду информации целесообразно относить любые сведения, разрабатываемые, исполняемые и передаваемы в органах внутренних дел, в основном, связана с взаимодействием сторонних организаций и правоохранительных органов: запросы, требования в информационный центр, в том числе поиск по базам данных, передачи сведений граждан и другая информация, попавшая в отделы Министерства Внутренних Дел.

Документы с пометкой «для служебного пользования» распространены не только в системе Министерства внутренних дел, но и в других организациях. Коммерческие предприятия используют информацию ограниченного распространения с целью защиты потенциально важной информации, относящейся к организации, от третьих лиц. Банки проставляют пометку «ДСП» на документах, содержащих информацию о потенциальных клиентах, системах и вкладах, чтобы защитить граждан от несанкционированного доступа к их персональным данным.

Сфера применения служебной информации ограниченного распространения достаточно широка, в связи с тем, что предприятия, организации, государственные и частные учреждения в своей повседневной деятельности используют информацию ограниченного распространения с целью защиты своих сведений, распространение которых может нанести им ущерб.

1.2. Классификация информационных рисков при работе со служебной информацией ограниченного распространения

Информация – это актив, который имеет ценность и должен быть защищен надлежащим образом. Информационная безопасность – это состояние информации, обеспечивающие ее защиту от широкого диапазона угроз с целью обеспечения уверенности в непрерывности работы, минимизации ущерба, реализации возможностей.

Информация может существовать в различных формах. Она может быть напечатана или написана на бумаге, создана в электронном виде, передаваться через сеть Интернет, по почте, нарочно, с использование электронных средств связи, выражаться устно. При этом, независимо от формы выражения или хранения она должна быть всегда защищена.

Сведения, процессы, связанные с информацией, информационными системами и сетевыми инфраструктурами являются существенными активами любой организации. В системе внутренних дел Российской Федерации информация требует более сильной защиты, в связи с потоком информации равных степеней секретности.

Предприятия, организации, государственные учреждения и структуры, их информационные системы и сети с каждым годом все чаще подвергаются различным угрозам безопасности, таким как шпионаж, компьютерное мошенничество, кража информации через несанкционированный доступ к компьютеру, социальная инженерия. Такие источники ущерба, как компьютерные вирусы, взлом и разного рода атаки (DoS-атаки, перехват трафика, сетевые черви, спам) становятся более распространенными, агрессивными и изощренными.

В современное время бумажная документация утрачивает свою актуальность, в связи с переходом на автоматизированные рабочие места. На ее замену приходит электронный документ, хранящийся на самой вычислительной машине, машинных носителях, в локальной сети или сети Интернет. Организация становится зависимой от информационных систем и услуг, что означает повышение уязвимости по отношению к угрозам безопасности.

В ходе анализа организаций, работающий с документами с пометой «для служебного пользования», было выявлено, что при проектировании многих информационных систем, вопросы безопасности не учитывались. Уровень безопасности, которой может быть достигнут техническими средствами, имеет ряд ограничений, в следствии чего, сопровождается надлежащими организационными мероприятиями, на которые, по статистике, не хватает материального обеспечения.

Деятельность организаций связана с получением, обработкой, хранением и передачей информации. При каждом взаимодействии со служебной информацией ограниченного распространения появляется угроза искажения информации. В аспекте информационной безопасности существует «информационный риск», который связан с нарушением одной или более базовых характеристик безопасности – конфиденциальности, целостности и доступности. Происходит снижение качества информации, приносящей ущерб предприятию.

Одним из необходимых аспектов нормального функционирования организации является обеспечение безопасности как земельной территории (охрана объекта), так и информации, циркулирующей на предприятии. В связи с этим, необходимо рассчитывать оценку риска, которая может произойти с информацией в процессе работы. Оценка риска – это систематический анализ:

1. Вероятного ущерба, наносимого организацией в результате нарушения информационной безопасности с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации и других активов.

2. Вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью.

Результаты этой оценки помогут в определении конкретных мер и приоритетов в области управления рисками, связанными с информационной безопасностью, а также внедрение мероприятий по управлению информационной безопасностью, с целью минимизации этих рисков.

Перед оценкой риска необходимо изучить классификацию существующих информационных рисков общего вида, которые делятся на основании нескольких критериев:

1. По источникам риска – внутренние и внешние.

Под внутренними угрозами понимается — угрозы безопасности информации, исполнителем которых является внутренний субъект, по отношениям к ресурсам организации (утечка информации, неавтоматизированный доступ)

Под внешними угрозами понимается – угрозы безопасности информации, инициатором которых является внешний по отношению к ресурсам организаций субъект (вредоносные программы, атаки хакеров, DoS-атаки, спам, фишинг, ботнеты).

2. По типам – естественные и искусственные.

К естественным относятся природные явления, которые не зависят от человека (ураганы, пожары, наводнения).

Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными.

3. По характеру могут быть – преднамеренными и непреднамеренными.

Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнании сотрудников.

Преднамеренные в отличии от предыдущих, создаются специально. Они могут быть организованны как сотрудниками организаций, так и третьими лицами.

4. Умышленные угрозы преследуют цель нанесения ущерба пользователями автоматизированной информационной системы и подразделяются на активные и пассивные.

Активные угрозы имеют цель нарушения нормального процесса функционирования систем посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. Источником таких угроз является действия нарушителей, программных вирусов.

Пассивные угрозы направлены на несанкционированное использование информационных ресурсов, при этом не оказывая влияния на их функционирование (прослушивание).

Данная классификация информационных ресурсов целесообразна для любой организации, в том числе и для системы Министерства внутренних дел Российской Федерации.

Разобравшись в видах риска, который может быть нанесен организации, следует проанализировать воздействие на информацию, которые могут произойти в следствии возникновения описанных выше информационных ресурсов.

1.3. Анализ воздействия на процесс обработки служебной информации ограниченного распространения

В основе любой деятельности, связанной с информационной деятельностью, лежат процессы, которые представляют собой совокупность последовательных действий (операций), производимых над информацией, с целью получения определенного результата. Информационные процессы могут быть разнообразными, но их все можно свести к трем основным видам: обработка, хранение и передача информации.

Обработка информации представляет собой целенаправленный процесс получения одних «информационных объектов» из других путем выполнения определенных алгоритмов. Для того, чтобы проанализировать воздействие на процесс обработки служебной информацией ограниченного распространения, необходимо разобраться в алгоритме, из которого состоит сама обработка информации.

Составим таблицу основных процедур при обработке данных:

Рис. 2. Процедуры обработки данных

Создание данных – как процесс обработки, предусматривает их образование в результате некоторого алгоритма и дальнейшее использование для преобразований на других уровнях.

Поиск информации осуществляется с целью набора данных для дальнейшего преобразования в единый смысловой структурный текст.

Модификация данных связана с отображением изменений в документе, осуществляемых путем включения новых данных, изменения уже существующих и удаление ненужных.

Создание документов заключается в преобразовании информации в формы, пригодные для чтения, как человеком, так и компьютером. В этом действие можно отнести также считывание, сканирование и сортировку документов.

И последнее, но самая важная процедура при обработке данных – это контроль безопасности: целостности, конфиденциальности (при необходимости), доступности, который направлен на адекватное отображение реального состояния информации, обеспечивая ее защиту от несанкционированного доступа, сбоев и повреждений при обработке с помощью технических и программных средств.

На стадии обработки информация подвергается значительным воздействиям. В каких-то случаях это изменения, которые вносятся санкционированно, с целью улучшения и модернизации информации, в других – изменения создают злоумышленники, не имеющие санкционированного разрешения на доступ к информации, с целью ее искажения, изменения, незаконного распространения, а главное – нанесение ущерба организаций для подрывания ее нормального функционирования.

Информация, обрабатываемая в организациях может осуществляться двумя способами: в бумажном виде, либо с помощью электронного носителя, откуда и вытекает разграничение воздействий, оказывающих на нее отрицательное влияние. В зависимости от источника и вида воздействия оно может быть непосредственным на защищаемую информацию либо посредственным, через другой источник воздействия.

Со стороны людей возможны следующие виды воздействия:

1. Воздействия на информацию при непосредственной работе с ней;

2. Воздействия на носители защищаемой (флеш – накопители, магнитные диски, бумажный носитель и др.);

3. Несанкционированное обращение по отношению к вычислительной технике на которой обрабатывается защищаемая информация;

4. Внесение фальсифицированной информации в документ;

5. Создание аварийных ситуаций для средств обработки информации;

6. Вмонтирование в ЭВМ разрушающих радио- и программных закладок;

7. Внедрение вирусных программ, способствующих дистанционному воздействию на обработку информации в онлайн режиме.

Со стороны техники:

1. Выход систем из строя:

- поломки, аварии (без вмешательства людей);
- возгорания, затопления;
- выход из строя источников питания;
- воздействия природных явлений.

2. Сбои в работе ЭВМ:

- появление технических неисправностей элементов систем;
- воздействия природных явлений;
- нарушения режима работы источников питания.

В основе любого дестабилизирующего воздействия лежат определенные причины, побудительные мотивы, которые обуславливают появление того или иного вида и способа воздействия. Вместе с тем и причины имеют под собой основания — обстоятельства и предпосылки, которые вызывают данные причины, способствуют их появлению. Однако наличие источников, видов, способов, причин и обстоятельств (предпосылок) дестабилизирующего воздействия на обработку информации ограниченного распространения представляет потенциально существующую опасность, которая может быть реализована только при наличии определенных условий для этого, которые создают, по статистике,

сами сотрудники организации, в силу своей невнимательности, халатности и корысти.

Исходя из вышеизложенного, служебная информация ограниченного распространения берет свое начало еще со времен зарождения присяги на верность царю и государству. До введения официального термина «государственная тайна», служебная информация имела особо важное значение в жизни государства, ведь именно от этих сведений и отношения к их важности зависело развитие как внешней политики государства, так и внутренней.

Сегодня информацию воспринимают как один из важных активов организаций, который имеет ценности и должен быть защищен. Однако учитывая особенность современного времени, когда информационные технологии становятся неотъемлемой частью как жизни людей, так и различных сфер деятельности, проблема защиты информации становится все более актуальной.

С каждым годом злоумышленники усовершенствуют свои подходы к получению информации противозаконными способами, пытаясь своими силами избежать наказания. Информация теряет свою ценность при несанкционированном распространении. В связи с этим, сотрудники предприятий должны быть грамотно обучены основам информационной безопасности, чтобы избежать самых обыденных и глупых ошибок.

2. Анализ и методы повышения безопасности при работе со служебной информацией ограниченного распространения

2.1. Угрозы информационных рисков служебной информации ограниченного распространения в системе Министерства внутренних дел Российской Федерации

Говоря о безопасности объекта (системы), подразумевается, что с помощью этого объекта или над этим объектом совершаются определенные действия. Если объект бездействует (не функционирует), не носит каких-либо ценности, то, соответственно, можно сделать вывод о нецелесообразности его безопасности.

Проблема изучения ситуации и факторов, которые могут представлять определенную опасность для информации, поиска и обоснования комплекса мер и средств по их исключению или снижению, характеризуются следующими особенностями:

1. Обширным количеством факторов характерных опасных ситуаций, необходимостью выявления источников и причин их возникновения.

2. Необходимостью выявления и изучения спектра возможных мер и средств, направленных на устранение угроз, с целью обеспечения безопасности.

Согласно ГОСТу Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: «Угрозы информационной безопасности представляет собой совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб или вред) для организаций». То есть угроза информации обусловлена вполне определенными факторами, которые могут сложиться в конкретной ситуации.

По отношению к информационной системе все множество угроз можно разделить на две группы: внешние и внутренние, каждая из которых, в свою очередь, подразделяется на умышленное и случайное, явные и скрытые.

Без этапа, на котором происходит выявление и анализ угроз защищаемой информации, нельзя говорить о безопасности построения информационной системы и о защите информации на предприятии. Для полного создания комплекса по защите информации, необходимо трактовать «информационную безопасность» не как узконаправленное понятие, а как широкое, подходящее для любой организации на территории всей страны. Согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года № 646, «Информационная безопасность Российской Федерации – это состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качества и уровень жизни граждан, суверенитет, территориальная целостность и устойчивая социально – экономическое развитие Российской Федерации, обороны и безопасности государства».

В современном мире информация – это не просто сведения, передаваемые между людьми, это орудие, халатное обращение с которым может привести к непоправимым последствиям. С данной точки зрения, система МВД РФ является одним из уязвимых мест, входящих в систему обеспечения безопасности России. В подразделениях Министерства Внутренних Дел происходит обработка информации разных степеней секретности, включающих: три грифа секретности – «особой важности», «совершенно секретно», «секретно»; пометку «для служебного пользования». Количество документов, имеющих грифы или пометку, обрабатываются во всех подразделениях Министерства Внутренних Дел, в связи с чем необходимо проанализировать возможную опасность при работе со сведениями, составляющими государственную тайну и служебной информацией ограниченного распространения.

Согласно целям организации защиты служебной информации ограниченного распространения, можно выделить следующие угрозы [3]:

1. Утечка, хищение служебной информации ограниченного распространения по техническим каналам.

2. Несанкционированное уничтожение, искажение, подделка, копирование, распространение, блокирование служебной информации ограниченного распространения.

3. Неправомерный или несанкционированный доступ к служебной информации ограниченного распространения.

4. Искажение полноты, целостности и достоверности служебной информации.

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный доступ лица к документированной информации и как результат – овладение этой информацией и противоправное ее использование. Целью и результатом несанкционированного доступа может быть не только овладение ценными сведениями и их использование в конкретных целях, но и их видоизменение, уничтожение, подмена и т. п.

Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, сотрудники, работающие конкретно с информацией, документами и базами данных. При этом надо иметь ввиду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а не из-за невнимательности и безответственности сотрудников.

Выделим несколько причин, по которым может произойти утрата информационных ресурсов ограниченного распространения:

1. При наличии интереса конкурента, учреждений, фирм или организаций конкретной информации.

2. При возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах.

3. При наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией. Эти условия могут включать:

− отсутствие системной аналитической работы по выявлению и изучению угроз, каналов и степени риска нарушения безопасности информации;

− неэффективную систему защиты;

− непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

− неупорядоченный подбор сотрудников и текучесть кадров, сложный психологический климат в коллективе;

− отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

− отсутствие контроля со стороны руководства организации за соблюдением сотрудниками требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

− бесконтрольное посещение помещений организаций посторонними лицами.

Каналы несанкционированного доступа могут быть двух типов: организационные и технические. Организационные каналы разглашения информации основаны на установлении разнообразных взаимоотношений Злоумышленника с организацией или ее сотрудникам для последующего несанкционированного доступа к интересующей информацией.

Основными видами организационных каналов могут быть:

1. Поступление злоумышленника на работу в организацию.

2. Установление доверительных взаимоотношений с сотрудниками организаций (подразделений).

3. Тайная или по фиктивным документам проникновение в здание, помещения, криминальный или силовой доступ к информации (кража документов, дисков, компьютеров, шантаж и склонение к сотрудничеству, подкуп сотрудников, создание экстремальных ситуаций и т. п.).

Широкие возможности несанкционированного получения сведений создает техническое обеспечение офисных технологий. Любая управленческая деятельность всегда связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализ ситуаций на ЭВМ (электронной вычислительной машине), изготовлением, размножением документов и т. п.

Технические каналы утечки информации возникают при использовании злоумышленником специальных технических средств, позволяющих получать защищаемую информацию без непосредственного контакта с сотрудниками организаций, документами, делами и базами данных.

Технический канал представляет собой физический путь утечки информации от источника к злоумышленнику. Канал возникает при анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, зрительную или иную форму отображения.

В результате эффективного использования каналов несанкционированного доступа к служебной информации ограниченного распространения и разнообразных методов ее добывания злоумышленник получает:

1. Подлинник или официальную копию документа (бумажную, электронную), содержащего информацию ограниченного доступа.

2. Несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т. п.)

3. Диктофонную, магнитофонную, видеокассету с записью текста документа, переговоров, совещаний.

4. Письменное или устное (лично, по телефону) изложение за пределами организаций содержание документа, ознакомление с которым осуществлялось санкционированно или тайно.

5. Аналог документа, переданного по факсимильной связи или электронной почте.

6. Речевую или визуальную запись текста, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирование с большого расстояния).

2.2. Роль субъективных факторов, воздействующих на безопасность информации при работе со служебными сведениями ограниченного распространения

В настоящее время на одном из первых мест в Министерстве внутренних дел Российской Федерации стоят вопросы развития и внедрения автоматизированных информационных систем в деятельности органов внутренних дел, в том числе применения пере-

довых подходов и технологий информатизации МВД России. Информатизация органов внутренних дел обусловлена спецификой деятельности по обеспечению общественной безопасности и правопорядка, основанной на формировании, хранении и использовании огромных массивов информации о гражданах, материальных объектах, правонарушениях и лицах их совершающих, о самих органах и подразделениях, их силах и средствах. Основной целью применения информационных технологий в деятельности органов внутренних дел является существенное повышение качества, изменение содержания и характера труда сотрудников. Благодаря автоматизации целого ряда информационных процессов, сотрудники органов внутренних дел освобождаются от рутинных, трудоемких операций, что, безусловно, увеличивает как производительность их деятельности, так и улучшает ее качество.

При этом в условиях продолжающегося масштабного развития ведомственной информатизации, осуществляемой во взаимодействии с планом развития информационно-телекоммуникационной инфраструктуры Российской Федерации, в МВД России существенно возрастают требования к подготовке кадров для подразделений органов внутренних дел. Одновременно улучшается оснащение этих подразделений современными образцами технических средств, эффективно эксплуатировать которые может лишь хорошо подготовленный сотрудник. Повышается необходимость формирования квалифицированного кадрового состава для четкого выполнения поставленных задач, а также сведения к минимуму количества ошибок и сбоев при внедрении и эксплуатации систем.

Особенностью профессиональной деятельности сотрудников органов внутренних дел Российской Федерации в информационных системах и телекоммуникационных сетях является то, что она строго регламентирована в соответствии возложенными на сотрудников функциональными задачами. Нарушения и отклонения от установленных правил и норм трактуются либо как умышленные действия, либо как непреднамеренные действия или случайные ошибки. Составляя два главных класса угроз безопасности, и те, и другие зачастую приводят к серьезным последствиям [14].

С учетом того, что используемые в органах внутренних дел информационные и телекоммуникационные системы и их элементы являются критичными для жизнедеятельности общества и государства, ущерб, наносимый этими нарушениями, может быть весьма существенен. Таким образом, существующая вероятность нарушений делает профессиональную деятельность сотрудников одним из уязвимых звеньев в ведомственных системах обработки и передачи информации, основанных на взаимодействии человека и машины. Кроме того, вопрос угрозы субъективного (человеческого) фактора особо остро встает в последние годы во время активного внедрения элементов подсистем информационной безопасности в системе Министерства внутренних дел Российской Федерации.

Субъективный или человеческий фактор является объектом изучения многих наук, что предопределило в конечном итоге появление междисциплинарных теорий, отражающих его сущностные характеристики [15]. При научном анализе такого явления, как человеческий фактор, возникает несколько существенных проблем. Во-первых, сам термин «человеческий фактор» многозначен по своему содержанию и его всестороннему изучению в том или ином виде посвящена практически вся социология. Во-вторых, подобное многообразие проявления «человеческого фактора» придает ему междисциплинарный характер и создает определенные трудности в выделении его в качестве отдельного направления для изучения. В-третьих, отсутствует (или является слишком абстрактной) общая теория человеческого фактора.

Большинство встречающихся в научной литературе интерпретаций понятия «человеческий фактор» сводятся к двум позициям: термин рассматривается как «процесс» или как «свойство» [17]. Позиция, рассматривающая человеческий фактор как процесс (субъектную деятельность) определяет его как «специфическое обозначение функционирования человека в системе социальных, экономических, производственных, научно-технических, организационно-управленческих и др. отношений». При рассмотрении же человеческого фактора как свойства, он определяется как «совокупность психологических, физиологических, антропометрических и других характеристик человека, его возможностей и

ограничений». Каждая из этих позиций, безусловно, имеет право на существование т.к. они в значительной степени дополняют друг друга, охватывая широкий спектр умышленных и ошибочных действий.

Классификация умышленных действий в целом весьма разнообразна и во многом зависит от профессионального статуса человека и занимаемой им должности. При этом не все из возможных действий распространяются на сотрудников органов внутренних дел в первую очередь вследствие их дисциплинированности.

Причины, способствующие ошибочным действиям человека, можно объединить в несколько групп [19]:

– недостаточность информационного обеспечения или его отсутствие. Особенно сильно эта проблема может проявляться в экстремальных ситуациях и в условиях дефицита времени на принятие решения во время несения службы;

– ошибки, вызванные воздействием внешних факторов (отвлечение внимания от возникшей проблемы);

– ошибки, вызванные физическим и психологическим состоянием и свойствами человека (внезапный стресс при общей монотонной работе, эмоциональная напряжённость, импульсивность или, наоборот, подавленная реакция на проблему);

– ограниченность ресурсов поддержки и исполнения принятого решения;

– отсутствие учёта человеческого фактора в списке возможных причин инцидента.

Сравнивая результаты аналитики одного из ведущих российских разработчиков систем защиты корпоративной информации InfoWatch за период времени с 2008 по 2018 год [16], можно утверждать, что рост угрозы со стороны человеческого фактора вырос практически втрое (с 30% до 85%).

К рассматриваемым в приведенных аналитических данных субъективным угрозам, в частности относятся:

- кража информации – 64%;
- вредоносное программное обеспечение – 60%;
- покушение на систему безопасности – 48%.
- спам – 45%;
- халатность сотрудников – 43%;

– аппаратные и программные сбои – 21%;
– кража оборудования – 6%;
– финансовое мошенничество – 5%.

Приведенные данные наглядно демонстрируют что, наиболее распространенными субъективными угрозами являются кража информации, вредоносное программное обеспечение и покушение на систему безопасности. Нельзя не отметить и высокий процент субъективных угроз, вызванных халатностью сотрудников.

В силу высокой проработанности вопросов организационного обеспечения деятельности сотрудников органов внутренних дел влияние данной проблемы на систему МВД России в целом минимально, однако проявления подобных ошибок, как показывает практика, имеют вовсе не нулевую вероятность, и этот факт побуждает оценить степень влияния и риск проявления подобных инцидентов. Одним из широко известных примеров подобного инцидента является проникновение 12 мая 2017 года в ведомственную сеть МВД вируса- шифровальщика WannaCry. По словам первого заместителя Министра внутренних дел Российской Федерации А.В. Горового из-за несоблюдения «правил пользования информационными системами» и «попытки присоединить служебный компьютер к Интернету» вирус атаковал ряд компьютеров ведомственной сети.

Анализируя общемировые показатели влияния на безопасность информации субъективного фактора по разным источникам можно выделить следующее соотношение [18]:

25% – непосредственное влияние через действия пользователей, специалистов по обеспечению работ, внешних лиц, заинтересованных в защищаемой информации;

75% – опосредованное влияние через созданную человеком автоматизированную информационную систему, используемую технологическую базу, а также через внешние, созданные человеком условия функционирования информационной инфраструктуры.

Можно увидеть, что субъективный фактор в своем деструктивном проявлении создает реальную повседневную угрозу информационной безопасности. Учитывая изложенное, очевидно,

что возникает потребность в проведении исследований, целью которых является изучение степени влияния субъективного фактора на функционирование защищаемого объекта, а также определение способов сведения до минимума рассматриваемой угрозы в системе Министерства внутренних дел Российской Федерации.

Проведенный анализ работы частных охранных структур и фирм, обеспечивающих внедрение и эксплуатацию информационных систем, задействованных для охраны объектов, позволил выделить основные субъективные риски. Размер выборки для изучения и анализа составил 800 человек сотрудников служб безопасности на 9 охраняемых объектах. Метод анализа апробирован. Основой метода являлись: опрос, тестирование, наблюдение.

Как основные выявлены следующие проблемы:

10,4% – неправильно контролируемый допуск (излишнее доверие, несоблюдение регламентов по отношению к проверяющим);

15% – неполное умение обращаться с оборудованием систем безопасности;

4,6% – полное неумение обращаться с оборудованием;

14% – неполное знание регламентов и правил.

1,3% – полное незнание регламентов и политики безопасности.

В 54,7% случаев за время анализа ошибок не выявлено.

Таким образом, в общей сложности 45,3% процентов исследуемых случаев в разной степени представляли собой угрозу для системы безопасности: либо из-за технических ошибок по вине персонала, либо из-за действий злоумышленников происходил отказ в обслуживании систем безопасности как на короткое, так и на длительное время.

Анализ основных причин проявления человеческих ошибок и методов их устранения, проведенный на основе наблюдений и подробного изучения организации безопасности внутри исследуемых объектов, позволил составить общие рекомендации, значительно снижающие вероятность реализации субъективных угроз:

1. Разработка методических рекомендаций, четких регламентов, подробных приказов, а также принятие зачетов и выполнение специально разработанных тестов;

2. Отведение большого количества часов на практику, закрепление навыков, отработка действий до автоматизма, разбор спорных ситуаций;

3. Регулярное тестирование систем безопасности: проведение специальных проверок, контрольное наблюдение;

4. Правильный анализ и качественная оценка рисков;

5. Исключение технической либо иной другой разведки по отношению к пунктам безопасности.

Помимо организационных моментов, имеющих повсеместную практику внедрения, снижение рисков информационной безопасности в деятельности сотрудников, вызванных субъективным фактором, в органах внутренних дел Российской Федерации представляется актуальным проведение следующих мероприятий:

1. Разработка и внедрение технологий, предназначенных для дистанционного и непосредственного наблюдения состояния сотрудника путем периодического измерения его биометрических параметров;

2. Электронная оценка и прогнозирование поведения сотрудников органов внутренних дел, а также иного персонала по обслуживанию объектов Министерства внутренних дел Российской Федерации: установка программного обеспечения и дополнительных видеокамер, фиксирующих пассивность и активность субъекта по ряду невербальных признаков.

Проведённый анализ трудовой и служебной деятельности, а также процессов эксплуатации и интегрирования информационных систем, предназначенных для обеспечения функционирования МВД России в рамках полномочий, позволяет установить, что степень влияния субъективного фактора сильно отличается от тенденций, наблюдаемых в коммерческих фирмах и иных негосударственных организациях. Несомненно, проявление человеческого фактора присутствует, но организационная политика служебных проверок и расследований позволяет выявлять инциденты, разбирать их коллегиально и предотвращать появление подобных ошибок.

2.3. Исследование подходов к анализу оценки информационных рисков

Стремительное развитие информационных технологий привела к значительному увеличению степени автоматизации процессов в современных организациях. Это связано с тем, что в современном мире прирост количества информации превратил ее из второстепенного ресурса в фактор, решающим образом, воздействующим практически на все сферы общественной жизни, отражая возрастающую информационную зависимость общества. Повсеместное применение вычислительной техники позволило выйти Министерству внутренних дел на новый, более качественный уровень, в достижении поставленных задач. Однако, в такой же степени, это стало и причиной многих сбоев, появления уязвимостей и многих других угроз информационной безопасности. Зависимость от информационных систем и технологий означает, что органы внутренних дел становятся более уязвимыми по отношению к угрозам различного рода, и потому, конфиденциальная информация, подобно любым другим видам защищаемой информации, нуждается в защите. Скоротечная модернизация информационных систем только усугубляет ситуацию. Огромное разнообразие техники, встроенных функций, но при этом отсутствие должной системы безопасности.

Анализ состояния дел в сфере оценки защищенности информационных ресурсов показывает, что злоумышленные действия над ними не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Все чаще реализуются такие угрозы как мошенничество, вредительство, промышленный шпионаж, компьютерные взломы, заражения компьютерных систем вредоносными программами и другое.

Увеличение объемов информации, хранимой в электронном виде, приводит к тому, что ее потеря или разглашение наносит существенные убытки подразделениям. Нарушение работоспособности информационных систем приводит к остановке рабочих процессов, что так же наносит ущерб. Современная рабочая си-

стема с каждым годом старается максимально исключить бумажный документооборот, регистрируя, сохраняя, создавая, передавая все документы одним способом и в электронном виде. В связи с этим, защита информации должна рассматриваться как неотъемлемая составляющая информационных систем современных организации, в особенности в системе Министерства внутренних дел.

В практической деятельности специалистами отмечаются большие проблемы, связанные с организационным направлением по достижению рискозащищенности информации. Имеющиеся проблемы связывают с отсутствием адекватной политики по обеспечению безопасности информационных систем, несоблюдение установленных правил, недостаток квалифицированных кадров. Проанализировав место и роль организационного направления в сфере обеспечения безопасности информации, стоит отметить, что в общем объеме мероприятий по достижению информационной защищенности организации нормативно-правовые меры составляют 5%, физические меры 15%, технические – 25–30%, организационные меры – 50%.

Несмотря на возрастающий интерес, проведение исследований, появление разработок в сфере оценки и управления информационной защищенностью, на данный момент в России противоречиво. С одной стороны, это связано с детальным изучением и проработкой вопросов технической и программно-аппаратной защиты информационных систем и крупными финансовыми вложениями в технические средства защиты. С другой стороны, обозначая значимость организационного направления в защите информационных систем, в нормативно-методической литературе и на практике отсутствуют четкие рекомендации и методические разработки по совершенствованию данной деятельности в Министерстве внутренних дел Российской Федерации, согласно появлению новых угроз, уязвимостей и других факторов, способных оказать дестабилизирующее воздействие на защищаемый ресурс.

Сегодня, в связи со стремительно меняющейся работоспособной средой, важнейшим условием в любой сфере деятельности становится способность руководителей предвидеть, оценить и ми-

нимизировать степень возникновения возможных рисков. В процессе оценки системы управления информационной защищенностью ключевыми элементами являются объективная идентификация и оценка наиболее значимых для системы информационных рисков, в результате которых будут расставлены приоритеты, определены требования к информационной безопасности.

Учитывая, что оценка информационных рисков представляет собой одно из важных направлений в достижении рискозащищенности органов внутренних дел и его подразделений, возникает необходимость в совершенствовании существующих методических подходов к оценке информационных рисков и создание новых, более организованных, качественных. Поэтому разработка и решение теоретических и практических проблем оценки информационных рисков на сегодняшний день является актуальной проблемой.

Исследование подходов к оценке рисков при работе со служебной информацией ограниченного распространения позволяет отметить, что многие из них рассматривают, в основном, технические и технологические аспекты, которые на сегодняшний день являются наиболее изученными и детально проработанными. Однако другие аспекты информационной безопасности, такие как постоянный контроль за функционированием всей системы защиты, включая персонал, оценку степени надежности персонала при работе со служебной информацией и так далее, зачастую выпадают из поля зрения сотрудников подразделений по обеспечению режима секретности.

Рис. 3. Модель взаимосвязей между составляющими элементами системы безопасности информационных ресурсов

Рассматривая деятельность по защите информации в Министерстве внутренних дел Российской Федерации, необходимо отметить, что она может структурно включать в себя следующие подсистемы:

- организационно-правовую защиту информации;
- инженерно-техническую защиту;
- программно-аппаратную защиту информации;
- криптографическую защиту информации;
- защиту информации в телекоммуникационных сетях и системах.

Структура системы защиты информационных ресурсов как подсистемы комплексной системы управления информационной безопасностью в органах внутренних дел отражена на рисунке ниже.

Рис. 4. Структура системы защиты информационных ресурсов в системе управления деятельностью территориальных органах

Любая система защиты информационных ресурсов территориального органа имеет свои особенности, но при этом должна отвечать общим требованиям:

– во-первых, система защиты информации должна быть предоставлена как нечто целое. Целостность системы будет заключаться в наличии единой цели функционирования, информационных связей между ее элементами, иерархичности построения подсистемы управления;

– во-вторых, она должна обеспечивать безопасность информационных ресурсов, средств их обработки и защиту интересов участников информационных отношений;

– в-третьих, система защиты, методы и средства должны быть по возможности легкими в пользовании, не создавая законному пользователю дополнительных неудобств, связанных с процедурами доступа к информации, и в то же время, быть непреодолимой преградой для несанкционированного доступа злоумышленника к защищенной информации;

– в-четвертых, система защиты должна быть экономически приемлема. Необоснованные траты на обеспечение безопасности могут стать угрозой функционирования безопасности, в связи с чем, они должны соответствовать степени опасности и стоимости защищаемых ресурсов.

Система защиты информации включает в себя совокупность элементов, ее образующих, и их свойства. Структурная часть системы составляет ее внутреннюю организацию, которая позволяет системе нормально функционировать, передавать информацию только по каналам, контролируемым системой. Вместе с тем, элементы имеют и внешние связи, которые решают поставленные системой задачи из вне – это функциональная часть системы. Обе части не отделены друг от друга. Это две стороны одних и тех же элементов, составляющих систему защиты информации.

В методологии защиты информационных ресурсов для противодействия многочисленным угрозам выделяются три основных направления обеспечения безопасности: правовое, организационное и инженерно- техническое. Каждое из направлений имеет свои особенности, методы и средства. Однако на практике применяется комплексный подход, включающий в себя три основных направления, с целью системного обеспечения надежности передаваемой, хранимой, обрабатываемой информации.

Анализ подходов к защите информации позволяет отметить, что большинство исследователей придерживаются комплексного подхода, однако есть среди них и те, кто отдает свое предпочтение структурному подходу, другие предлагают применять объектно-ориентированный подход.

Исследование современных подходов защиты при работе со служебной информацией ограниченного распространения показывает актуальность применения комплексной системы защиты информации, соединяющих в себе локальные систем в единое целое.

Важный аспект применения комплексного подхода состоит в том, что он технологически должен строиться таким образом, чтобы сами процессы защиты носили регулярный характер и охватывали все этапы функционирования системы, кроме того, обеспечивали защиту как циркулирующей информации, так и ее носителей на всех стадиях сбора, хранения, обработки и передачи при всех режимах функционирования Министерства внутренних дел.

Задачи, решаемые в комплексной системе защиты информационных ресурсов, можно разделить на 3 типа: задачи анализа, синтеза и управления. Задачи анализа включают характеристики объекта и цели его функционирования, цели организации системы защиты, состав средств и затрат. Задачи синтеза – проектирование архитектуры схем функционирования объекта и системы. К задачам управления относится поиск управляющих воздействий на параметры объекта и системы с целью поддержания их в требуемом состоянии. Все эти задачи решаются в процессе проектирования, которое проходит система и объект защиты, и жизненного цикла: создание, функционирование, совершенствование.

Всю совокупность требований при организации защиты в Министерстве внутренних дел условно можно разделить на три группы: общие требования, специальные требования и требования к отдельным компонентам (под системами и средствами защиты, документационному обеспечению и другому).

К общим требованиям относятся:

1. Технические – использование технических средств и организация их эксплуатации в соответствии со стандартами по защите информации;

2. Организационные – полнота контроля выполнения поставленных задач, удовлетворение в методическом, информационном и кадровом обеспечении;

3. Экономические – предусматривают решение совокупности задач защиты при оптимальном расходовании ресурсов, наличие резерва средств совершенствования системы защиты;

4. Эргономические – обеспечение психологической совместимости работы персонала с техническими средствами, установка оптимального режима работа.

Среди специальных требований выделяют:

1. Влияние факторов внешней среды и особенностей территориального подразделения;

2. Выбранная стратегия защиты при обосновании ресурсного обеспечения, необходимого для организации защиты;

3. Неопределенности при организации процессов функционирования (вероятностный характер угроз, сбоев в работе средств защиты, действий нарушителей, ошибок в работе сотрудников и тому подобное).

Для каждой подсистемы определяются требования в виде перечня обеспечиваемых функций защиты, основных характеристик этих функций, перечня средств, реализующих эти функции. Состав требований к средствам и техническому обеспечению формируются исходя из различных параметров: место применения, способ использования, размер контролируемой зоны, проведение специсследований и спецпроверок с целью определения величины показателей защищенности по соответствующим методикам и с учетом реальной обстановки на территории.

Для успешного функционирования системы защиты информационных ресурсов, следует обратить внимание на первоначальный, базовый элемент обеспечения защищенности – определение общей стратегии и деятельности по управлению рисками. Это позволяет гарантировать, что информационная безопасность серьезно рассматривается на различных организационных уровнях объекта.

Рассмотрев своевременные методические подходы к обеспечению защиты служебной информации ограниченного распространения, следует помнить, что пристальное внимание в изучении и на практике уделяется комплексной системе защиты информационных ресурсов, которая должна обеспечивать использование всех средств и методов при разработке защиты, таких как формы проявления уязвимости информации, объекты защиты, цели и задачи защиты, факторы и обстоятельства, влияющие на организацию и функционирование системы информационной защищенности Министерства внутренних дел.

2.4. Методика оценивания информационных рисков при работе со служебной информацией ограниченного распространения

На сегодняшний день безопасность является ключевым вопросом при внедрении и использовании электронных систем. В органах внутренних дел активно используются информационные технологии, а сама информация является важнейшим объектом. В связи с этим возникают риски, присущие деятельности Министерства внутренних дел – риски, связанные с нарушением информационной безопасности (информационные риски).

Наибольшую сложность при управлении информационными рисками представляет выбор методики, по которой оценивается риск. С одной стороны, не существует как такового программного комплекса, который бы удовлетворял по всем параметрам, с другой – руководство органов внутренних дел зачастую не выделяет на это достаточное количество времени и денег.

Говоря об оценке риска, стоит помнить, что уровень риска зависит от вероятности реализации определенной угрозы в отношении определенного объекта, а также величины возможного ущерба. Таким образом, суть управления рисками состоит в оценке их размера, выработке эффективных и экономических мер их снижения, а также в установлении приемлемых рамок для них. Следовательно, управление рисками включает в себя два вида деятельности, которые циклически чередуются:

1. Оценка (переоценка) рисков;

2. Выбор эффективных и экономически выгодных средств защиты (нейтрализация риска).

Учитывая существенную разнотипность источников и видов угроз, разработка методик и алгоритмов оценки риска – достаточно трудоемкая и значимая задача для любой информационной системы, требующей выполнения ряда условий.

1. Необходимо построение гибкой модели информационной системы, ее комплексное описание, с учетом программных, аппаратных ресурсов, внутренних и внешних угроз и уязвимостей, способных подстраиваться особенностям системы Министерствам внутренних дел.

2. Учитывая значительное количество факторов риска, математическая модель оценки информационной безопасности, должна допускать разработку эффективных численных алгоритмов обработки информации в моделях.

3. Должна быть предельно понятная методика оценки рисков, чтобы владелец информации мог оценить применимость и эффективность методики к конкретной информационной системе.

Для оценки рисков информационной безопасности важно выделить и проанализировать все, или по крайней мере, основные угрозы и уязвимости, через которые возможна реализация угроз, и которые могут воздействовать на информационную тему с целью снижения ее работоспособности. На сегодняшний день существует ряд методик оценки информационных рисков информационной безопасности, к основным из которых можно отнести:

1. Метод оценки рисков, основанный на построении модели угроз и уязвимостей.

Данная методика основана на использовании преимущественно экспертной и статистической информации об угрозах и уязвимостях. Для оценки рисков в информационной системе определяется защищенность каждого отдельного ценного ресурса при помощи вероятностей реализации угроз, действующих на конкретный ресурс (вероятность сбоев в работе программно-аппаратных комплексов, некомпетентность сотрудников и тому подобное), а также уязвимостей, через которые эти угрозы могут быть реализованы. Полученная оценка вероятностей позволит ранжировать угрозы и уязвимости по степени риска.

2. Метод оценки рисков, основанный на построении модели информационных потоков.

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Рассматривая средства защиты ресурсов с ценной информацией, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации.

Для начала следует описать архитектуру сети:

1. Все ресурсы, на которых хранится ценная информация.

2. Сетевые группы, на которых хранится ценная информация (то есть физические связи ресурсов друг с другом).

3. Виды ценной информации (по грифа и пометкам).

4. Ущерб для каждого вида ценной информации по видам угроз.

5. Группы пользователей, имеющих доступ к ценной информации.

6. Характеристики этого доступа (вид и права)

7. Средства защиты информации

8. Средства защиты рабочего места.

Исходя из введенных данных, можно построить полную модель информационной системы, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Риск оценивается отдельно по каждой связи «пользователь» – «информация», то есть модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики.

Риск реализации угрозы информационной безопасности для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность.

Расчет рисков по трем видам основных угроз:

1. Определяем вид доступа пользователя (сотрудника) к информации.

2. Определяем права доступа пользователя (сотрудника) к информации.

3. Вероятность реализации угрозы зависит от класса пользователя. Например, автоматизированный пользователь, а именно тот, который имеет персональный доступ к рабочему месту, имеет меньшую угрозу, чем сотрудник, не санкционировано использующий компьютерный ресурс.

4. Особым видом средства защиты является специально созданный программно-аппаратный комплекс, использующийся в Министерстве внутренних дел.

В итоге, чтобы получить риск для ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

В системе органов внутренних дел наибольшую защиту информации обеспечивают программно-аппаратные комплексы, на которых происходит вся работа с секретной документацией: создание, обработка, хранение передача, печать и копирование.

Изучив организационные особенности обеспечения безопасности информации в органах внутренних дел, можно прийти к неудовлетворительным результатам, согласно которым на одно структурное подразделение приходится один программно-аппаратный комплекс. Казалось бы, проблемы никакой нет, однако стоит учитывать количество сотрудников подразделения, которым необходимо работать с данным комплексом. Так, например, в подразделении уголовного розыска числится двенадцать оперативных сотрудников, каждый из которых работает с документами ограниченного доступа. Обработка подобных документов возможна только на компьютерном аппаратном средстве, предназначенном для обработки, хранения информации, содержащей сведения ограниченного доступа. Согласно этому расчету на двух сотрудников должно приходиться одно специализированное рабочее место, как минимум.

В системе Министерства внутренних дел таким средством является программно-аппаратный комплект «Панцирь – М», созданный на базе операционной системы «Linux», которая защищена от несанкционированного доступа системой «Страж КТ» 3.0 (сертификат ФСТЭК № 2145). В комплекте содержит дополнительное оборудование: лазерный принтер, который защищен колбами, источник бесперебойного питания, системный контейнер с накопителем на жестком магнитном диске, встроенный генератор шума «ГШК – 180» для защиты от утечки информации за счет ПЭМИН (сертификат ФСТЭК №1672), электронный ключ (идентификатор пользователя). В соответствии с технологическим процессом, все компоненты, устанавливаемые в «Панцирь – М» до сборки, приходят специальные проверки. После сборки «Панцирь – М» проходит тестирование трехсуточным технологическим прогоном и специальными исследованиями на ПЭМИН. Средняя стоимость данного программно-аппаратного комплекса составляет 67 тысяч 429 рублей.

На данный момент разграничение доступа при работе с документацией ограниченного доступа в системе органов внутренних дел не совершенно. В связи с этим, предлагается рассмотреть методику работы для выявления угроз и уязвимостей при работе со служебной информацией.

Повышение качества работы с информацией связано с понижением информационных рисков при обработке служебной информации ограниченного доступа. Воздействия на информацию

определяются с помощью таких способов как наблюдаемость, идентифицируемость и управляемость. Наблюдаемость подразумевать процесс, с помощью которого можно прямо или косвенно определить по внешним параметрам воздействие на информацию, идентифицируемость – возможность предсказать воздействие в будущем, а управляемость представляется процессом, где в некоторый момент времени воздействие на информацию может быть переведено из управляющего состояния в управляемое.

Для качественного анализа воздействий на процессе обработки служебной информации ограниченного распространения необходимо:

- установить цели и область применения
- идентифицировать риск
- проанализировать риск
- провести сравнительную оценку риска
- создание вариантов борьбы с риском

Установление цели и области применения	- внутренние цели -внешние цели -разработка критериев
Идентификация риска	- Что может произойти? - Когда и где? - Как и почему?
Анализ риска	- идентификация средств управления - определение последствий событий - оценка вероятности событий - количественная оценка риска
Сравнительная оценка риска	- сравнение с критериями - расстановка приоритетов - сравнение преимуществ и неблагоприятных моментов
Вариация борьбы с риском	- анализ и оценка результатов - идентификация вариантов - оценка вариантов - подготовка и выполнения плана по борьбе с рисков

Рис. 5. Схема разработки по борьбе с угрозами.

Для успешной разработки политики безопасности в организации необходимо определить мероприятия по управлению информационной безопасностью, которые включают:

– наличие документа, описывающего политику информационной безопасности;

– распределение обязанностей по обеспечению информационной безопасности;

– обучение вопросам информационной безопасности;

– информирование об инцидентах, связанных с информационной безопасностью.

Перечисленные мероприятия применимы для большинства организаций и информационных сред. Следует отметить, что, хотя все приведенные мероприятия являются важными, уместность какой-либо меры должна определяться исходя из конкретных рисков, с которыми сталкивается организация.

Информация стала залогом успешного функционирования Министерства внутренних дел, поддержания его нормального развития. Однако широкое использование информации породило новый вид рисков – информационные риски, которые могут составлять серьезную угрозу развитию, функционированию и защищенности системы органов внутренних дел. Поэтому информационные риски требуют незамедлительного выявления, анализа и оценки в целях недопущения несанкционированного доступа к служебным сведениям ограниченного распространения и их утечки. Необходимо помнить, что формулирование и осуществление политики безопасности по устранению любых подобных рисков не будет эффективной, если существующие шаблоны и правила используются не так, как должны, что происходит из-за необученности сотрудников или их неосведомленности о важности проблемы. Именно поэтому работы по обеспечению информационной безопасности должны быть комплексными. Управление информационными рисками – субъективный, сложный и очень важный процесс в деятельности подразделений органов внутренних дел, особенно в части касающейся работы со сведениями, содержащими государственную тайну и со служебной информацией ограниченного распространения, когда вероятность ущерба для Министерства внутренних дел очень велика.

Несмотря на то, что в настоящее время разработано множество систем и методик по расчету и анализу возможных информационных рисков, которые позволяют оперативно информировать об их появлении и соблюдать основные правила информационной безопасности – конфиденциальность, целостность и доступность, следует учитывать сторонние факторы, возникающие конкретно из определенных особенностей расположения и функционирования конкретного территориального органа системы Министерства внутренних дел России.

3. Организация работы со служебной информацией ограниченного распространения в системе Министерства внутренних дел России

3.1. Обеспечение информационной безопасности при работе со служебной информацией в органах внутренних дел

В современном мире, выстроенном на повсеместном применении компьютерной техники, совсем поменялся подход к пониманию информации. Появление вычислительных машин информация начал восприниматься как одна из неотъемлемых составляющих жизни любого человека. Наряду с этим, взгляд на информацию изменился от восторженного до обыденного.

Информацию можно разделить на правовую и неправовую. Первая бывает нормативная и ненормативная.

Нормативная формируется в последовательности правотворческой деятельности и содержится в нормативных правовых актах. К ней относятся Конституция РФ, Федеральные конституционные законы, Федеральные законы, Законодательные акты субъектов РФ, Указы Президента РФ, Постановления Правительства РФ, разнообразные нормативные акты органов исполнительной власти всех уровней, акты органов местного самоуправления.

Ненормативная формируется в порядке правоприменительной и правоохранительной деятельности. С ее помощью исполнятся предписания нормативных правовых актов. Такая информация подразделяется на несколько больших групп:

1. Информация о состоянии законности и правопорядка:

2. Информация о гражданско-правовых отношениях, договорных и иных обязательствах (договоры, соглашения и т. п.).

3. Информация, представляющая административную деятельность органов исполнительной власти и местного самоуправления по исполнению нормативных предписаний.

4. Информация судов и судебных органов (судебные дела и судебные решения).

5. Правоохранительная информация.

Как видим, информационная безопасность органов внутренних дел- это состояние защищенности интересов ОВД в информационной сфере в соответствии с возложенными на них задачами.

Существенные элементы информационной сферы:

1. ведомственная информация и информационные ресурсы;

2. ведомственная информационная инфраструктура – средства и системы информатизации;

3. субъекты исполнения информационной деятельности – сотрудники органов внутренних дел;

4. система нормативно-правового регулирования.

К особо значимым объектам обеспечения информационной безопасности в правоохранительной и судебной сферах можно отнести:

1. ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, которые содержат сведения и оперативные данные;

2.информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

3. информационная инфраструктура.

Наибольшую опасность, в правоохранительной и судебной сферах, несут внешние и внутренние угрозы.

Ко внешним относятся:

– разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, которые занимаются сбором сведений о раскрытии задач, планов деятельности, методов работы и мест дислокации специальных подразделений и органов внутренних дел;

– функционирование иностранных государственных и частных коммерческих структур, старающихся обрести несанкционированный доступ.

Внутренними, являются:

– срыв установленного регламента сбора, обработки, хранения и передачи информации, хранящейся в картотеках и автоматизированных банках данных и применяющейся для расследования преступлений;

– дефицит законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

– отсутствие целостной методологии сбора, шлифовки информации, а также хранение информации криминалистического, статистического и оперативно-розыскного характера;

– сбои программного обеспечения в информационных системах;

– умышленные поступки, а также погрешности персонала, работающего над и ведением картотек и автоматизированных банков данных.

Безопасность информационных ресурсов и информационной инфраструктуры органов внутренних дел выражается через безопасность их наиболее важных свойств. Так как субъектам информационных отношений урон может быть причинен воздействием на процессы и средства обработки критичной для них информации, то полной необходимостью становиться обеспечение защиты всей системы информации от незаконного вторжения, способов хищения и/или разрушения любых компонентов данной системы в процесс ее деятельности.

Безопасность каждого компонента автоматизированной системы (АС) формируется из обеспечения трех его характеристик:

- конфиденциальности, которая заключается в доступности только тем субъектам (пользователям, программам, процессам), у которых имеются особые полномочия.

- целостности – свойство информации, характеризующееся умением противостоять несанкционированному или непроизвольному истреблению, или искажению.

- доступности, получить доступ к необходимому компоненту системы при наличии соответствующих полномочий возможно в любое время без особых проблем.

Нарушение таковых характеристик, представляет собой угрозы для информационной безопасности органов внутренних дел.

Необходимо подчеркнуть, что важнейшей целью защиты АС и, соответственно вращающейся в ней информации выражается в предотвращение или минимизация наносимого ущерба, а также разглашения, искажения, утраты или противозаконного тиражирования информации.

Средствами обеспечения информационной безопасности – это совокупность правовых, организационных и технических средств, предназначенных для обеспечения информационной безопасности. (5)

Все средства обеспечения информационной безопасности можно разделить на две группы:

- формальные – это средства выполняющие свои функции по защите информации формально, то есть главным образом без участия человека.

- неформальные это те, основу которых составляет деятельность людей.

Формальные средства делятся на физические, аппаратные и программные.

Физические – механические, электрические, электронные, электронно-механические и устройства и системы, которые работают автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

Аппаратные –встраиваемые в аппаратуру системы обработки данных намеренно для решения задач по защите информации.

Так, наряду с вышеперечисленным, проводиться ряд мероприятий, необходимых для реализации защиты информации. К ним относятся такие:

– Распределение и замена реквизитов разграничения доступа (паролей, ключей шифрования и т. п.).

– Мероприятия по пересмотру состава и построения системы защиты.

– Исполняемые при кадровых изменениях в составе персонала системы.

– По подбору и расстановке кадров (контроль принимаемых на работу/службу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, организация условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т. д.).

– Противопожарная охрана, охрана помещений, пропускной режим, меры по обеспечение сохранности и физической целостности техники и носителей информации и т. п.

– Открытая и скрытая проверка за работой персонала системы.

– Проверка за использованием мер защиты.

– Мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации.

И еще ряд других мероприятий, направленных на защиту информации ограниченного доступа. Помимо организационных мер, немаловажную роль имеют всевозможные меры технического характера (аппаратные, программные и комплексные

В органах внутренних дел уделяется особое внимание вопросам сохранности тайных сведений, выработки у работников большой бдительности. Тем не менее отдельными из них часто недооценивается тяжесть утечки таких сведений. Они проявляют недобросовестное отношение и халатность при обращении с секретными документами, и это часто ведет к разглашению тайных сведений, а порой к потере секретных изделий и документов. При этом некоторыми работниками поддерживают сомнительные связи, разглашают важные сведения о методах и формах работы органов внутренних дел. Низкие профессиональные качества некоторых работников часто ведут к нарушению конспирации проводимых мероприятий.

Оценка информационных рисков при работе со служебной информацией ограниченного распространения является неотъемлемой частью работы каждого организатора или предпринимателя, который работает с данными, имеющими ограниченное распространение. Оценка информационных рисков представляет собой процесс определения и анализа потенциальных угроз безопасности информации и разработки и применения соответствующих мер по их предотвращению и минимизации. При оценке информационных рисков нужно учитывать не только технические, но и организационные аспекты системы безопасности информации.

Оценка информационных рисков для служебной информации ограниченного распространения требует анализа всех возможных угроз безопасности информации, которые могут повлиять на безопасность данных и информационных систем организации. В этой связи при оценке информационных рисков необходимо про-

вести анализ следующих аспектов: состояние оборудования и систем информационной безопасности; уровень защиты данных от несанкционированного доступа; уровень организационных и технических мер по защите данных; процессы управления информационной безопасностью; используемые информационные технологии; источники и методы распространения информации; потенциальные угрозы внешней или внутренней информационной безопасности; уровень подготовки работников и потребителей информации; и другие факторы.

Для проведения оценки информационных рисков при работе со служебной информацией ограниченного распространения организации должны применять различные методики анализа информационных рисков, включая анализ угроз, анализ потенциальных уязвимостей и анализ рисков. На основе результатов этих анализов организация может разработать проекты по предотвращению и минимизации информационных рисков, а также принять меры для мониторинга и устранения угроз безопасности.

Таким образом, оценка информационных рисков при работе со служебной информацией ограниченного распространения – это важная задача для каждой организации, которая занимается обработкой и хранением данных, имеющих ограниченное распространение. Она позволяет организации лучше понимать свои информационные риски и принимать меры по их предотвращению, а также по повышению уровня безопасности.

До начала работ по оценке рисков необходимо определить, в качественных или количественных показателях выражать риски.

Качественная оценка рисков позволяет выявить существующие риски и определить степень их воздействия.

Существуют несколько моделей качественной оценки. Все они достаточно просты, варианты различаются лишь числом градаций шкал. Одна из самых распространенных моделей – трехуровневая. Каждый фактор оценивается по шкале «низкий – средний – высокий».

Во многих случаях трехуровневая шкала является достаточной, но в некоторых случаях может потребоваться более детальная шкала, например пятиуровневая: «незначительный – низкий – средний – высокий – очень высокий». Однако следует помнить:

какой бы уровень детализации ни был выбран, необходимо позаботиться о том, чтобы интерпретация уровней могла отражать различия между уровнями.

Трехуровневые качественные шкалы для оценки возможного ущерба, вероятности реализации угроз, величины рисков предлагают использовать большинство международных стандартов. Основное преимущество качественного подхода состоит в том, что данный подход позволяет отказаться от сложных процедур определения точной стоимости актива, затрат на защитные меры, вероятности реализации угроз, что значительно сокращает время на проведение работ по оценке рисков. Однако полученные результаты субъективны, не имеют однозначной интерпретации.

Итоговые результаты качественной оценки рисков могут служить исходной информацией для проведения количественной оценки.

Методы количественного характера выражают риски численно, т. е. ожидаемые потери в числовом эквиваленте и вероятность или частоту этих потерь. В результате количественной оценки каждому риску ставится в соответствие величина возможных финансовых потерь в случае его реализации, что может использоваться для обоснования необходимости внедрения защитных мер, а также рассчитывается вероятность реализации угроз, что позволяет оценить их реальную опасность.

Количественные оценки позволяют оценить соотношение возможных финансовых потерь и расходов на приобретение и эксплуатацию защитных мер, а затем рассчитывать экономический эффект мероприятий.

Однако у описанного подхода есть несколько существенных недостатков. Во-первых, не существует эффективного формализованного метода, позволяющего точно определить стоимости активов. Во-вторых, реализация всех аспектов количественного подхода требует больших затрат.

Количественная оценка точнее, позволяет получить конкретные значения рисков, но требует заметно больше времени и ресурсов, что не всегда оправданно, так как организации постоянно раз-

виваются, изменяются, следовательно, за то время, пока выполняется оценка, фактические значения рисков могут оказаться другими.

Какой метод оценки рисков выбрать, зависит от того, насколько точно можно рассчитать стоимость объектов защиты, оценить вероятность реализации угрозы и степень уязвимости. Если эти данные точны и достаточны, то целесообразно использовать количественную оценку, в противном случае – качественную. Как уже было отмечено ранее, для количественной оценки рисков нужна достоверная, полная исходная информация, которую, как правило, сложно получить. Например, для оценки вероятности угроз необходима накопленная статистика, отражающая факты и частоту реализации угроз. К сожалению, отсутствие исходной информации и эффективного инструментария ее обработки делает использование количественных методов оценки в настоящее время неэффективным.

3.2. Базовая и детальная оценка рисков информационной безопасности

Выбор глубины проводимой оценки рисков будет зависеть от множества факторов: область деятельности, размеры организации, степень автоматизации бизнес-процессов, уровень зрелости организации, наличие квалифицированного персонала, средств, выделяемых на обеспечение ИБ. Анализ перечисленных факторов позволяет выбрать подходящий в каждой конкретной ситуации подход к оценке рисков.

Существует три подхода к оценке рисков информационной безопасности:

– базовый;

– детальный;

– комбинированный.

Первый подход предполагает обеспечение базового уровня защищенности путем выбора минимального набора защитных мер. В данном случае оценивают вероятности нарушения безопасности и тяжести возможных последствий такого нарушения. При

этом риск тем больше, чем выше вероятность нарушения безопасности и тяжесть возможных последствий. Основное преимущество использования базового подхода – это возможность обойтись минимальным количеством ресурсов при проведении оценки и дальнейшей обработки рисков ИБ. Рассматриваемый подход экономически эффективен при условии, что выбранный базовый уровень защищенности соответствует уровню, необходимому для большинства объектов защиты организации. Если выбранный базовый уровень завышен, то защитные меры окажутся излишними, в случае же если базовый уровень защищенности занижен, то для ряда объектов защиты выбранные меры будут недостаточны.

Если базовых оценок недостаточно, используют детальную оценку рисков. В этом случае для каждого объекта защиты или группы объектов защиты определяют перечень актуальных угроз и оценивают вероятность их реализации, а также степень легкости, с которой угрозы могут реализоваться, т. е. уровень уязвимости. Описываемый подход позволяет определить необходимые и достаточные защитные меры, однако связан со значительными затратами времени и средств, а также с необходимостью привлечения квалифицированных специалистов. Поскольку оценка проводится одинаково тщательно для всех объектов защиты организации, определение и реализация необходимых защитных мер для какого-либо критичного объекта защиты может произойти слишком поздно, когда безопасность уже нарушена и организация несет убытки. Таким образом, проводить детальную оценку рисков применительно ко всем объектам защиты не рекомендуется.

У каждого из перечисленных подходов есть достоинства и недостатки, в связи с чем в каждом конкретном случае важно найти между ними баланс.

В качестве такого баланса выступает третий подход – комбинированный, который предполагает проведение предварительной оценки для всех объектов защиты, с тем чтобы установить, какой из подходов (базовый или детальный) лучше подходит для конкретного объекта защиты (или группы объектов защиты).

Исходные данные для принятия решения о применимости базового или детального подходов могут быть получены в результате анализа следующих факторов:

– требования нормативно–правовых актов РФ по информационной безопасности;

– цели, для достижения которых используется объект защиты (если в организации выделены и описаны бизнес–процессы, то указываются бизнес–процессы, в реализации которых задействован объект защиты);

– степень зависимости деятельности организации от объекта защиты;

– стоимость создания, приобретения объекта защиты, затраты на поддержание в рабочем состоянии, ремонт и т. д.;

– наличие потенциальных нарушителей (конкуренты, обиженные сотрудники и т. п.);

– возможность возникновения экстремальных погодных условий, близость к источникам опасности и т. д.

Если нарушение безопасности объекта защиты может причинить организации ущерб, отрицательно повлиять на ее деятельность, репутацию, то принимается решение проводить детальную оценку рисков, во всех остальных случаях достаточно применение базового подхода.

Использование быстрой и простой предварительной оценки рисков в значительной мере способствует успешному планированию работ по оценке рисков, ресурсы и средства могут быть вложены туда, где они принесут максимальный эффект, так как они в первую очередь будут направлены на критичные объекты защиты, в наибольшей степени нуждающиеся в защите.

Единственный потенциальный недостаток такого подхода состоит в следующем: отдельные объекты защиты могут быть ошибочно отнесены к объектам защиты, не требующим проведения детальной оценки рисков, и к этим объектам защиты в дальнейшем будут применены базовые защитные меры.

Подобный подход наиболее предпочтителен для большинства организаций, так как сочетает лучшие свойства базового и детального подходов и позволяет при сведении к минимуму времени и усилий, затраченных на оценку рисков, обеспечить необходимую защиту критичных объектов защиты.

Определение величин, формирующих значение рисков, как правило, осуществляется методом экспертных оценок, который

предусматривает формирование мнения группы экспертов, являющихся специалистами в рассматриваемой предметной области, путем их опроса.

На качество полученных оценок существенно влияют полнота и достоверность предоставляемой эксперту исходной информации. Для этих целей создается экспертная комиссия, в состав которой могут входить как сотрудники организации, так и сторонние эксперты. В организации разрабатывается положение, регламентирующее деятельность экспертной комиссии.

Такой подход не требует значительных средств или времени, однако оценки субъективны, основаны на практическом опыте конкретного эксперта, и это влечет за собой трудности при обосновании перед высшим руководством необходимости реализации выбранных защитных мер.

3.3. Проблемные вопросы, связанные с деятельностью по обработке служебной информации ограниченного распространения сотрудниками органов внутренних дел

Вместе с сотрудниками Главного управления Министерства внутренних дел России по Краснодарскому краю, а именно управлением делопроизводства и режима, были обозначены проблемы, с которыми сотрудники органов внутренних дел сталкиваются в повседневной деятельности. В ходе обсуждения были выделены обоснованные предложения по созданию и внедрению примерного перечня служебной информации ограниченного распространения, указаны проблемные аспекты, присутствующие в приказе Министерства внутренних дел России от 9 ноября 2018 года № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России».

Для проведения анализа, в ходе которого была выявлена актуальность, распространения в деятельности сотрудников различных подразделений Министерства внутренних дел России, был со-

ставлен небольшой опрос, из которого можно сделать вывод о полезности предлагаемых изменений, который состоит из следующих вопросов:

1. Как часто вы работаете со служебной информацией ограниченного распространения?

2. Как часто вы являетесь исполнителем документа с пометкой «Для служебного пользования»?

3. С какими трудностями вы сталкиваетесь будучи исполнителем документа с пометкой «Для служебного пользования»?

4. Какие наиболее типичные угрозы могут появиться при работе со служебной информацией ограниченного распространения? (при передаче, обработке и хранении).

5. На сколько процентов, по вашему мнению, защищен процесс работы со служебной информацией?

6. Считаете ли вы полезным разработанные рекомендации для сотрудников, работающих с документами ограниченного распространения?

7. Помог ли вам в повседневной деятельности разработанный Перечень документов при работе со служебной информацией ограниченного распространения?

8. Помимо приказа Министерства внутренних дел России № 755 от 9 ноября 2018 г. «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России» знакомы ли вы с другими нормативными правовыми актами в сфере работы со служебной информацией?

9. Какой приказ был наиболее полезным при работе со служебной информацией ограниченного распространения: 825 дсп или 755? Почему?

Опрос был проведен среди 50 сотрудников из следующих подразделений: дежурная часть, управление делопроизводства и режима, управление организации охраны общественного порядка, управление экономической безопасности и противодействия коррупции и штаб.

В ходе проведенного опроса были проанализированы ответы сотрудников подразделений. На основе ответов были сделаны выводы о проблемах, возникающих при работе со служебной информацией ограниченного распространения.

Сотрудники опрощенных подразделений работают со служебной информацией как минимум 1 раз в день; включая: прием, обработку, хранение и передачу. Исполнителями документа они могут быть до 3 раз в месяц. Самыми главными трудностями, с которыми сталкиваются опрошенные – отсутствие перечня сведений, которым необходимо присваивать ограничительную пометку. Отсутствие в приказе конкретного алгоритма работы со служебной информацией ограниченного распространения. Среди наиболее типичных угроз, при работе со служебной информацией ограниченного распространения, выделены:

1. Несанкционированный доступ к информации.
2. Обработка информации на неаттестованных по требованиям безопасности информации на средствах электронно-вычислительной техники.
3. Несанкционированное изготовление светокопий документов.

На вопрос о процентной защищенности процесса работы со служебной информацией можно сделать вывод о халатном отношении к документам с пометкой «Для служебного пользования», игнорирования необходимости проставления пометки, неосознанность важности сведений.

Рекомендации способствуют повышению уровня грамотности сотрудников в сфере служебной информации, определению правил, регламентирующих работу со служебной тайной, требований и порядка обработки конфиденциальных сведений.

В повседневной деятельности сотрудникам был полезен разработанный Примерный перечень документов при работе со служебной информацией ограниченного распространения. Проводя аналогию между утратившим силу приказом Министерства внутренних дел России № 825 дсп и приказом Министерства внутренних дел России № 755, сотрудники выделяют различные положительные особенности у каждого из нормативных правовых документов. Приказ Министерства внутренних дел России №755 более

подробно расписывает порядок работы со служебной информацией ограниченного распространения, но в нем отсутствует Примерный перечень. Приказ Министерства внутренних дел № 825 дсп наоборот, предусматривал Примерный перечень сведений, которым необходимо присваивать пометку «Для служебного пользования», но не освещает многие аспекты порядка работы со служебной документацией.

Исходя из полученных результатов опроса и совместного обсуждения с сотрудниками различных подразделений предлагаемых изменений, можно сделать вывод о целесообразности, актуальности, а главное необходимости внедрения результатов работы как предложению по усовершенствованию защиты документов с ограничительной пометкой в системе Министерства внутренних дел Российской Федерации.

Практическая деятельность сотрудников органов внутренних дел во многих аспектах связана с приемом, обработкой, передачей и хранением документов различных степеней секретности и ограничительного доступа. Для обеспечения защиты системы Министерства внутренних дел России в целом, необходимо уделять особое внимание созданию условий, способствующих безопасному обращению с ограничительной документацией. В связи с недостаточной грамотностью сотрудников, работающих с документами ограничительного распространения, нами были составлены и разработаны документы, способствующие усовершенствованию и облегчению работы сотрудникам, а также внушению и объяснению работникам о важности документов, с которыми им приходится работать в повседневной деятельности. Примерный перечень служебных сведений ограничительного распространения, рекомендации для сотрудников по работе со служебной информацией оказались актуальными необходимыми разработками для системы Министерства внутренних дел Российской Федерации

Деятельность сотрудников органов внутренних дел напрямую связана с получением, передачей и хранением сведений ограниченного распространения. Как говорилось в первой главе работы, – служебная информация не относится к сведениям, составляющим государственную тайну, однако, к ней нет свободного доступа на основании требований федеральных законов, приказов

Министерства внутренних дел. Служебная информация ограниченного распространения обладает действительной или потенциальной ценностью, в силу ее неизвестности лицам, не имеющим права доступа к ней, и по отношению к которой, в системе Министерства внутренних дел, принимаются правовые, организационные, технические и иные меры защиты информации.

15 декабря 1997 года в Министерстве внутренних дел России был принят приказ № 825 дсп, который содержал в себе условия отнесения информации к служебной тайне, примерный перечень служебных сведений ограниченного распространения и документов, их содержащих, образующихся в деятельности органов внутренних дел, образовательных и научно- исследовательских учреждений Министерства внутренних дел России, который состоял из следующих пунктов:

1. Протоколы и стенограммы заседаний коллегии, совещаний, конференций, научно-технических, методических, научных и других советов и комиссий Министерства внутренних дел России, органов внутренних дел, подразделений, учреждений, организаций и предприятий системы Министерства внутренних дел России, в ходе которых обсуждаются вопросы, содержащие сведения ограниченного распространения.

2. Документы (докладные записки, справки, акты и тому подобное), содержащие обобщенные сведения о фактическом положении дел и различным направлениям оперативно-служебной деятельности.

3. Документы по выполнению законодательных и иных нормативных правовых актов Российской Федерации, приказов Министерства внутренних дел России с ограничительными грифами.

4. Положение о структурных подразделениях, должностные инструкции сотрудников, деятельность которых связана с проведением работ закрытого характера.

5. Материалы по изучению и внедрению передовых форм и методов работы по направлениям оперативно-служебной деятельности, поименованным настоящим Примерным перечнем.

6. Планы (работы, перспективные, производственные и прочие) по выполнению мероприятий конфиденциального характера.

7. Акты (докладные записки, справки) по вопросам проверки наличия секретных документов и обеспечения режима секретности и конспирации.

8. Суточные сводки о происшествиях по Министерству внутренних дел, Главным управлениям внутренних де, управлениям внутренних дел, управлениям внутренних дел на транспорте.

В настоящее время на смену вышеизложенному приказу был издан приказ Министерства внутренних дел России от 9 ноября 2018 года № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России», в котором отсутствует Примерный перечень сведений и документов ограниченного распространения.

В повседневной профессиональной деятельности сотрудники полиции, а именно исполнители документов, сталкиваются с вопросами, касающимися отнесения сведений к служебной информации ограниченного распространения. Согласно приказу Министерства внутренних дел России от 9 ноября 2018 года №755, должностные лица, принявшие решение об отнесении информации к разряду ограниченного доступа, несут персональную ответственность за обоснованность (целесообразность) принятого решения и за соблюдение соответствующих ограничений. В связи с этим, руководители и сотрудники подразделений Министерства внутренних дел России, не имея хотя бы Примерного перечня информации, которую разрешено относить к ограниченному распространению, имеют затруднения в части, касающейся проставления на документе пометки «Для служебного пользования», согласно информации, которая в нем содержится.

Исходя из полученного практического опыта, сотрудниками отдела режима Главного управления Министерства внутренних дел по Краснодарскому краю, был разработан Примерный перечень служебной информации ограниченного распространения, который содержит совокупность направлений, содержащих информацию, распространение которой может нанести ущерб органам внутренних дел.

1. Протоколы заседаний, коллегий, совещаний, касающихся конкретных мероприятий по борьбе с преступностью.

Протоколы совещаний, на которых обсуждаются новые методики системной деятельности государственных и общественных органов, направленной на осуществление оперативно-розыскной деятельности, активного противостояния преступности.

2. Положения для оперативных подразделений.

В связи с тем, что оперативными подразделениями выполняются негласные мероприятия с целью выявления, пресечения и раскрытия преступлений, поиска скрывающихся и пропавших без вести людей, добычи информации о событиях и деяниях опасных для государства, целесообразно было бы на положениях о структурных оперативных подразделениях проставлять пометку «Для служебного пользования».

3. Должностные инструкции оперативных сотрудников Министерства внутренних дел России.

Большая часть деятельности оперативных сотрудников связана с документами, имеющими грифы «Секретно» и «Совершенно секретно». В связи с чем, целесообразно было бы отнесение их должностных инструкций к разряду информации ограниченного распространения.

5. Схемы расположения режимных кабинетов в территориальном органе.

В режимных помещениях осуществляется работа с информацией, содержащей сведения, составляющие государственную тайну. Несанкционированное воздействие преступников на кабинеты такого рода может нанести большой вред как отделу, так и Министерству внутренних дел в целом.

6. Персональные данные сотрудников Министерства внутренних дел Российской Федерации.

Любую персональную информацию, касающуюся сотрудника органов внутренних дел, целесообразно использовать с пометкой «Для служебного пользования».

8. Порядок проведения штабных учений (приказ, план, результаты).

В ходе проведения штабных учений (в случае, если информация будет общедоступной), преступники, наблюдая за действиями сотрудников подразделений Министерства внутренних дел, при

подготовке противоправных деяний, могут рассчитать порядок организации действий личного состава органов внутренних дел, что может привести к менее успешной ликвидации преступников.

9. Мероприятия по планированию действий сотрудников органов внутренних дел по охране общественного порядка.

10. Заключения и материалы служебных проверок по вопросам оперативно-розыскной деятельности и защиты государственной тайны в случае, если в них отсутствуют сведения, составляющие государственную тайну.

11. Заключение по результатам психофизиологического исследования (полиграф).

Отчет по итогу полиграфического исследования состоит из вопросов, которые были заданы человеку в течение всего опроса. Исходя из этого можно проанализировать алгоритм работы полиграфа, с целью лучшей подготовки преступников к исследованию.

12. Запросы, задания на проведение проверок в отношении лиц на наличие/отсутствие оперативной информации.

13. Запросы и ответы на проверку по учетам (Главный информационно-аналитический центр, информационный центр и другие).

При составлении примерного перечня были учтены все практические проблемные вопросы сотрудников, касающиеся подготовки документации.

Сотрудники органов внутренних дел выделяют еще одну существенную проблему при работе со служебной информацией ограниченного распространения. В территориальные органы Министерства внутренних дел поступают документы с пометкой «Для служебного пользования» не только из других подразделений органов внутренних дел, но также из органов исполнительной власти, организаций, не входящих в систему Министерства внутренних дел. Проблемный вопрос заключается в неопределенности изданного приказа Министерства внутренних дел России от 9 ноября 2018 г. №755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России» в части касающейся снятия копий и производства выписок с документа с пометкой «Для служебного пользования».

В ходе обсуждения проблемного вопроса, был изучен приказ Министерства внутренних дел Российской Федерации № 755 на наличие ответов по постановленному проблемному вопросу. Согласно пункту 30, главе 3 вышеуказанного приказа, «тиражирование документов (в том числе правовых актов Министерства внутренних дел России), содержащих служебную информацию ограниченного распространения, снятия с них копий и производство распространения, снятия с них копий и производство выписок осуществляется с письменного разрешения руководителя (начальника) органа, организации, подразделения системы Министерства внутренних дел России или уполномоченного им лица в порядке, предусмотренном пунктами 31 и 32 настоящей Инструкции». В данном пункте содержится обобщенное понятие документа с пометкой «Для служебного пользования», подлежащего тиражированию, снятию копий и производству выписок, не проводя градацию на поступившие из системы Министерства внутренних дел или из иного органа исполнительной власти.

Рассмотрим пункт 32 настоящей Инструкции: «с документов, содержащих информацию ограниченного распространения, поступивших в орган, организацию, подразделение системы Министерства внутренних дел России, списанных в дело или находящихся на архивном хранении, а также с отдельных экземпляров тиражированных документов осуществляется снятие копий или производство выписок из них». Ознакомившись с данным пунктов, приходим к выводу об отсутствии желаемой конкретики органа отправителя документа.

При дальнейшем изучении приказа рассмотри главу 4 пункт 40: «поступившие в органы, организации, подразделения системы Министерства внутренних дел Российской Федерации документы, содержащие служебную информацию ограниченного распространения, подготовленные в других органах и организациях, не подлежат передаче третьим лицам...». Как видно из пункта, определяется связь с другими органами, не входящих в систему Министерства внутренних дел Российской Федерации, однако, как и в других пунктах решения поставленной проблемы не отражено.

Исходя из вышеизложенного анализа приказа Министерства внутренних дел Российской Федерации № 755, вытекает вывод об

отсутствии порядка снятия копий и производства выписок из документов, поступивших из органов, организаций, подразделений, не относящихся к системе Министерства внутренних дел России. В связи с этим, предлагаем следующее решение: добавить в приказ Министерства внутренних дел России от 9 ноября 2018 г. №755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России» в главу 3 пункт, содержащий следующее:

«с документов, содержащих информацию ограниченного распространения, поступивших в орган, организацию, подразделение системы Министерства внутренних дел России из органов, организаций, подразделений, не входящих в систему Министерства внутренних дел России, осуществляется снятие копий и производство выписок с разрешения руководителя (начальника) органа Министерства внутренних дел России».

Еще одним проблемным вопросом, касающегося работы со служебной информацией ограниченного распространения, является введение в эксплуатацию в систему программно-аппаратного комплекса «Панцирь-М» мандатного управления доступом.

Мандатное управление доступом (Mandatory access control, MAC) – это система разграничения доступа на основе уровня доступа субъекта (конфиденциально, секретно, совершенно секретно, особой важности) и защитной метки объекта. Смысл в том, что субъект может получить доступ к тем объектам, у которых метка безопасности имеет тот же уровень или ниже, что и у объекта.

Субъект – это пользователь (сотрудник), а если быть точнее – процесс, который он инициализирует.

Объект – это файл, программа, база данных и любой из ее объектов, даже сетевой пакет.

Также предусмотрена иерархическая структура уровней доступа (особой важности, совершенно секретно, секретно, для служебного пользования).

Всем субъектам и объектам назначаются так называемые метки – значение уровня доступа у субъекта и значение уровня конфиденциальности объекта.

Каждый раз, когда субъект запрашивает объект происходит проверка соответствия меток и принимается решение о разрешении или запрете доступа. Так как структура уровней доступа иерархическая, то субъект имеет доступ к объектам соответствующего уровня конфиденциальности, а также ко всем другим уровням, находящимся по иерархии ниже. Проверка уровня доступа – это вертикальная безопасность, но в мандатной системе разграничения доступа предусмотрена и горизонтальная. В дополнение к уровням безопасности, существуют категории. Благодаря им можно разграничивать доступа среди субъектов с одинаковым уровнем доступа.

Субъекты не могут наделять правами доступа другие субъекты. Это может делать либо специальное лицо, обладающие знаниями о необходимых правах для пользователь (как правило сотрудник безопасности).

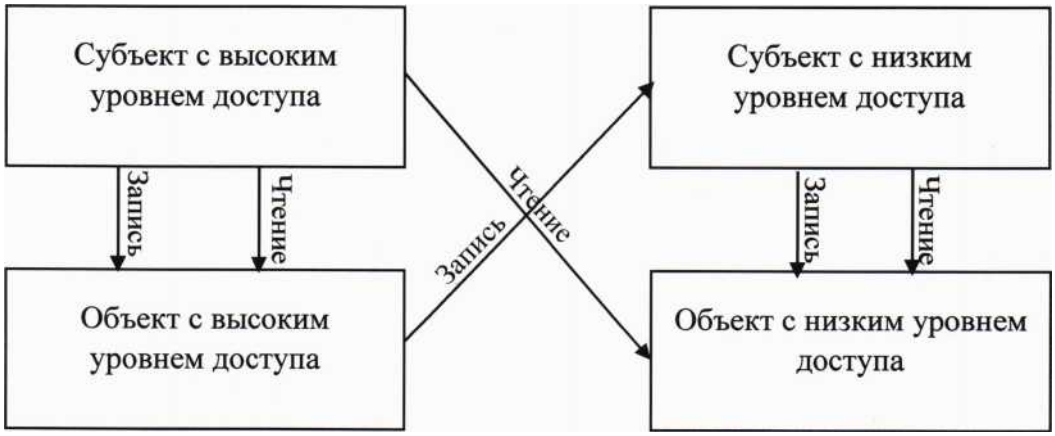

Рис. 6. Мандатная система разграничения доступа.

Из схемы видно, что субъект с высоким уровнем доступа имеет право на запись и чтение объекта с высоким уровнем конфиденциальности. Он также может читать документы с более низким уровнем конфиденциальности, но не изменять. В свою очередь субъект с низким уровнем доступа может читать и записывать в объект с низким уровнем конфиденциальности. Чтение объектов с высоки уровнем конфиденциальности ему запрещено, но разрешена запись (в том случае, если у сотрудника есть допуск по соответствующей форме, и он является исполнителем документа).

Хоть данная схема и предусматривает возможность субъектом с низким уровнем доступа записи данных в объект с высоким уровнем секретности, фактически с высоким уровнем секретности, фактически это не работает, так как «секретные» файлы, не будут видны в каталоге.

Как и любая система безопасности, мандатная система разграничения доступа имеет свои плюсы и минусы:

Плюсы:

1. Высокая степень надежности. Практически исключен взлом.
2. Автоматизированная проверка и обеспечение прав доступа.
3. Данные не могут быть изменены несанкционированно.

Минусы:

1. Требует много планирования.
2. Так как система мандатного разграничения доступа громоздкая, администраторы сильно загружены. Необходимо проверять назначение прав доступа.
3. Долгий и дорогостоящий процесс перехода на данную систему.

Изначально мандатное управление доступом было реализовано в специальной операционной системе Windows. Среди отечественных операционных систем мандатное разграничение поддерживается в Astra Linux Special Edition. Мандатное управление доступом в России является отличительной чертой систем защиты Государственной тайны. Astra Linux Special Edition соответствует всем требованиям к системам, обеспечивающим защиту конфиденциальных данных. Поэтому, на сегодняшний день, происходит усиленное внедрение в систему Министерства внутренних дел компьютеров «Мирт», на основе операционной системы Astra Linux.

3.4. Рекомендации сотрудникам, работающим со сведениями ограниченного распространения

Сегодня большинство организаций как системы Министерства внутренних дел, так и сторонних предприятий используют многоуровневые системы обработки информации – компьютеры, облачные хранилища, корпоративные сети и так далее. Все эти системы не только передают данные, но и являются средой их возможной утечки. Утечка секретной информации – это процесс неконтролируемого разглашения сведений, важных для организации.

Первая и самая основная причина, зародившаяся еще в древние времена – человека. В нашем случае, это сотрудники подразделений Министерства внутренних дел России. Каждый из сотрудников является потенциальной угрозой для безопасности информации. Часто люди забирают работу домой – перемещают рабочие файлы на свои флеш-носители, передают их по незащищенным каналам соединения, обсуждают информацию с сотрудниками других подразделений, халатно относятся к своей работе и своим обязанностям.

Действия сотрудников бывают умышленными и непреднамеренными. Непреднамеренные действия – это следствие незнания регламента работы со служебной информацией ограниченного распространения.

Риск утечки информации от сотрудников был, есть и будет. Его нельзя полностью исключить. Служба безопасности может принять меры, которые ограничат взаимодействие работников со служебной информацией ограниченного распространения:

1. Разработка правил разграничения доступа.
2. Соблюдение норм документирования информации.
3. Оперативное выявление сотрудников, которые несут разглашение данных.

В практической деятельности сотрудники проявляют халатность по отношению к работе со служебной информацией ограниченного распространения. В частности, оставляют свои пароли от учетных записей, записанные на листочке, прикрепленным к рабочему столу или на сам монитор; в блокноте, который лежит всегда на видном месте и другое.

Одну из важных угроз, связанных с человеком, представляет социальная инженерия. При слове «киберопасность» большинство руководителей думает о том, как защититься от хакеров, использующих технические уязвимости сетей. Но много кто забывает о том, что есть и другой способ проникнуть в организации и сети – через человеческие слабости. Это и есть социальная инженерия: способ обманом заставить кого-то раскрыть информацию или предоставить доступ к сетям данных. В случае социальной инженерии мошенники манипулируют людьми, чтобы получить от них информацию или доступ к ней.

Атаки с использованием социальной инженерии бывают разными:

1. «Ловля на живую». «Ловец» оставляет приманку – например, флешку с вирусом. Нашедший ее сотрудник, из любопытства, вставляет флешку в свой компьютер, и вирус поражает систему

2. «Претекетинг». Злоумышленник использует предлог, чтобы привлечь внимание жертвы и заставить ее сообщить информацию.

3. «Ты – мне, я – тебе». Многие социальные инженеры убеждают своих жертв в том, что те получат что-то в обмен на данные или доступ к ним (как показывает практика, чаще всего награда – материальные блага).

4. Взлом электронной почты и рассылка по контактам. Злоумышленник взламывает почту человека или его учетную запись в социальной сети, получая доступ к его контактам. Теперь от имени жертвы он может сообщить им, что его ограбили, и попросить перечислить ему денег или разослать ссылку на вредоносное ПО или клавиатурный шпион под видом интересного видео.

«Охота» и фарминг. И наконец, несколько более продвинутых методов социальной инженерии. Большинство простых методов, описанных выше, являются формой «охоты». Все просто: проникнуть, захватить информацию и убраться восвояси. Однако некоторые социальные инженеры налаживают связь с жертвой, чтобы получить больше данных за более длительный период времени. Этот метод известен как фарминг и представляет для злоумышленника повышенный риск разоблачения. Но в случае успеха он также дает гораздо больший «урожай».

Рис. 7. Жизненный цикл социальной инженерии.

Социальным инженерам особенно сложно противостоять, поскольку они используют особенности человеческой натуры – любопытство, уважение к властям, желание помочь друг другу.

В системе Министерства внутренних дел России, для защиты от несанкционированного доступа, при обработке или хранении служебной информации ограниченного распространения рекомендуем проведение следующих организационных мероприятий:

1. Выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите.

2. Определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право представлено.

3. Установление и оформление правил разграничения доступа, то есть совокупности правил доступа субъектов к объектам защиты.

4. Ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации.

5. Получение от объекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

На основании вышеизложенного, руководителям подразделений органов внутренних дел следует уделять особое внимание к отбору сотрудников, их качественным характеристикам.

Настоящее поколение достигает огромных высот в сфере развития информационных технологий. Изобретаются новые, многофункциональные средства вычислительной техники, которые работают как сам, так и с помощью человека. Доверия такого, какое предполагалось, к таки системам человечество не имеет в связи с тем, что компьютер – несовершенная машина, которая может иметь сбои в работе. Как бы современное поколение не относилось к средствам вычислительной техники, человек, по своей безопасности, ничем не уступает им. Что человек, что машина – несовершенные создания, доверие к которым нужно доказать.

Правила информационной безопасности для организации не самые сложные, но степень ответственности сотрудников не всегда гарантирует их безусловное выполнение. Это значит, что внедрение правил должно сопровождаться мотивационными мерами, стимулирующими их выполнение, и депремированием, дисциплинарной ответственностью в случае невыполнения.

Информирование сотрудников, как средство минимизации рисков в области информационной безопасности.

Первым правилом ИБ в организации должно стать информирование сотрудников. Инсайдерские утечки данных не менее опасны, чем внешние нападения. Сотрудник уголовного розыска, увольняясь, может уности сведения из оперативных и справочных учетов. О размере риска говорит объем рынка даркнета, измеряемый сотнями миллионов долларов в год только для российских ресурсов. Известный российский рынок торговли краденой информацией, Hydra, даже собирался провести ICO.

Всем пользователям информационной системы должны быть известны простые правила безопасности:

– использовать и периодически менять сложные пароли, никогда не передавать средства идентификации – пароль и логин – другим сотрудникам;

– не хранить в «облаках» конфиденциальную информацию, даже если нужно поработать с годовым отчетом из дома;
– уничтожать ненужные документы в шредере;
– не передавать информацию без официального запроса;
– не смешивать корпоративную и личную почту;
– архивировать важные файлы;
– блокировать компьютер перед уходом с рабочего места;
– уметь распознавать фишинговые письма;
– ознакомиться с практиками социальной инженерии и не поддаваться им.

Тестирование в игровой форме на знание правил информационной безопасности на предприятии позволит превратить теоретические сведения в сложившиеся навыки. Вторым важным способом поддержания необходимого уровня информационной безопасности в организации станет контроль доступа.

Правила контроля доступа и комплексного подхода в обеспечении информационной безопасности.

Контроль доступа реализуется на физическом, аппаратном и программном уровнях. Действует правило: никто не должен иметь больше привилегий, чем допускается его должностной инструкцией. Юристу не нужен доступ к бухгалтерским программам, а программисту – к чату руководства. Системные администраторы должны реализовать дифференцированную модель доступа, назначив каждому пользователю и группе пользователей роль, при которой доступными ему окажутся только определенные файлы и ресурсы. То же относится к правам администраторов.

Правило комплексного подхода должно стать незыблемым для системных администраторов и разработчиков структур информационной безопасности. Невозможно устранять уязвимости и недочеты частичными решениями, латая прорехи одну за другой до тех пор, пока администрирование системы станет невозможным. Необходимо с самого начала выстраивать информационную безопасность как единую с систему с учетом возможностей ее роста и прогнозированием направлений дальнейшего развития. Система должна включать единый комплекс организационных, технических и программных средств и контролироваться как единое целое.

Иные средства минимизации рисков информационной безопасности:

Системы мониторинга активности и обнаружения угроз**.** Наибольшие риски несут сотрудники-инсайдеры, допущенные к управлению и использующие съемные устройства, которые могут быть заражены вирусом. Но если система подключена к ведомственной информационной системе, возможны внешние риски. Системы мониторинга ограничены в функционале, они не могут блокировать действия пользователей. Они способны только отслеживать всплески подозрительной активности и уведомлять о них по заданному алгоритму. Их функции:

– обнаружение внешних атак и аномалий в поведении элементов сети;

– мониторинг инцидентов информационной безопасности;

– пассивный анализ уязвимостей;

– анализ конфигураций оборудования, правил доступа сетевого оборудования;

– контроль целостности данных и программного обеспечения.

Системы анализируют сетевые потоки, выявляют аномалии и неизвестные IP-адреса, атаки на незапротоколированные ранее уязвимости.

Системы предотвращения угроз. Эти программные средства носят проактивный характер: они не только информируют, но и действуют. В основном они управляют доступом пользователей, имея полномочия на блокировку неавторизованных действий. В случае неопределенной трансакции они вправе запросить ее авторизацию у руководителя более высокого уровня и в его отсутствие блокируют операцию..

Заключение

Оценка информационных рисков при работе со служебной информацией ограниченного распространения является определяющим фактором в вопросах обеспечения информационной безопасности как системы МВД России, так и для государства. Поэтому проблема, рассмотренная в работе, является актуальной в настоящий период времени. Исходя из этого можно с уверенностью отметить, что проведение мероприятий и внедрение изменений по улучшению работы со служебной информацией ограниченного распространения будет способствовать укреплению информационной безопасности подразделений системы Министерства внутренних дел Российской Федерации и государства в целом. Таким образом, решенные в ходе исследования теоретические и практические задачи, позволили выявить ряд проблем в изданном приказе Министерства внутренних дел России от 9 ноября 2018 года №755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России», а также в деятельности подразделений Министерства внутренних дел России и предложить меры по повышению уровня информационной безопасности.

Во-первых, предлагается создать систему мандатного разграничения доступа на объектах информатизации ОВД. Данная система поможет обеспечить безопасное обращение с документами различных грифов секретности и пометкой ограничительного доступа.

Во-вторых, предлагается внедрить в систему Министерства внутренних дел России разработанный примерный перечень служебных сведений ограниченного распространения, который поможет сотрудникам в процессе создания документов с ограничительной пометкой «Для служебного пользования».

В-третьих, в процессе работы были посещены различные подразделения Главного управления Министерства внутренних дел России по

Краснодарскому краю с целью получения эмпирических данных и изучения методики работы со служебной информацией

ограниченного распространения. Ввиду сложности создания копий документов, поступивших из организаций, предприятий, учреждений, не входящих в систему Министерства внутренних дел России, предлагается внести изменения в приказ Министерства внутренних дел России № 755, что позволит более эффективно работать со служебной информацией, а также осуществлять деятельность, связанную с обеспечением информационной безопасности.

Проведенный в работе анализ позволяет более конкретно определить систему мер по повышению уровня информационной безопасности в Министерства внутренних дел России по сокращению информационных рисков, при работе со служебной информацией ограниченного распространения. Вместе с тем, мы не претендуем на абсолютно законченное решение поставленных проблем. Однако результаты проведенного исследования могут в дальнейшем использоваться для более глубоких научных изысканий в области подразделений Министерства внутренних дел России и обеспечения их информационной безопасности.

Литература

1. Конституция Российской Федерации. Принята всенародным голосование 12 декабря 1993 г. (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 27 июня 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Указ Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера».

4. Указ Президента Российской Федерации от 17.03.1997 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

5. Постановление правительства Российской Федерации от 03.11.1994 №1233 (ред. От 06.08.2020) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».

6. Приказ Министерства внутренних дел России от 09.11.2018г. №755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе Министерства внутренних дел России».

7. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

8. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации.

9. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уроки целостности систем и программных средств.

10. Бескид П.П., Силин П.И. Управление информационными рисками: базовые понятия, классификация, стандартизация [Электронный ресурс] – https://www.elibrary.ru/item.asp?id=28202076 – статья в Интернете.

11. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им С.Ю. Вите. Серия 3: Образовательные ресурсы и технологии. 2015 №1 (9). С. 73-79.

12. 1. ГОСТ 34.321-96 Информационные технологии (ИТ). Система стандартов по базам данных. Эталонная модель управления данными – docs.cntd.ru [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200017662/

13. Смолян Г.Л., Солнцева Г.Н. Человеческий фактор в обеспечении безопасности информационной инфраструктуры // Сборник: Проблемы управления информационной безопасностью. Институт системного анализа РАН. 2002. – 224 с.

14. Тиц С.Н. Человеческий фактор [Электронный ресурс]: электрон. учеб. пособие / Самар. гос. аэрокосм. ун-т им. акад. С. П. Королева – Самара: Изд-во СГАУ, 2012

15. Глобальное исследование утечек информации в I полугодии 2018 года // InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/globalnoe-issledovanie-utechek-informatsii-v-i-polugodii-2018-goda. – Режим доступа: https://www.infowatch.ru/analytics/reports

16. Будников С. А., Паршин Н. В. Информационная безопасность автоматизированных систем: учебное пособие / Центр повышения квалификации специалистов по технической защите информации (ЦПКС ТЗИ). – Воронеж: Изд-во им. Е. А. Болховитинова, 2009. – 287 с.

17. Еркин А. В. Человеческий фактор в обеспечении информационной безопасности автоматизированной системы электронного документооборота: теория и практика проявления // Уральский институт управления – филиал РАНХиГС. Вопросы управления. 2011. № 3. С.31-39.

18. Корнаев Н.В. Учёт влияния субъективного фактора на защиту информации при внедрении и эксплуатации информационных систем в деятельности органов внутренних дел Российской Федерации // Сборник: Информационные технологии, связь и защита информации МВД России – 2017 С. 60-62.

Оглавление

Учебное издание

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ПРИ РАБОТЕ СО СЛУЖЕБНОЙ ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

Учебное пособие

Составители:
Ледовская Маргарита Александровна
Богданова Кристина Николаевна

В авторской редакции
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1918-5

Подписано в печать 28.02.2023. Формат 60х84 1/16.
Усл. печ. л. 4,5. Тираж 50 экз. Заказ 114.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.