Краснодарский университет МВД России

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ДЕЛОПРОИЗВОДСТВА И РЕЖИМА

Материалы
Всероссийской научно-практической конференции
(23 октября 2024 г.)

Краснодар
2025

УДК 316.485.6+004.7
ББК 66.4(0)+304.1
О-641

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Организация деятельности подразделений делопроизводства
О-641 и режима [Электронный ресурс] : материалы Всерос. науч.-практ. конф., 23 окт. 2024 г. / редкол.: А. В. Еськов, А. С. Победа, А. А. Датиев и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2025. – 1 электрон. опт. диск.

ISBN 978-5-9266-2151-5

В сборнике представлены материалы Всероссийской научно-практической конференции «Организация деятельности подразделений делопроизводства и режима», состоявшейся в Краснодарском университете МВД России 23 октября 2024 г.

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

УДК 316.485.6+004.7
ББК 66.4(0)+304.1

ISBN 978-5-9266-2151-5

Оглавление

Еськов А.В. Применение метода экспертных оценок для принятия решений сотрудниками отдела делопроизводства и режима…… 4

Звонарева А.Ю. О проблемных вопросах координации деятельности в сфере защиты государственной тайны, документационного обеспечения управления и рассмотрения обращений…… 9

Федченко А.Д. Актуальные вопросы цифровизации документационного обеспечения в органах внутренних дел…….. 13

Черкашина А.В. Проблемные вопросы в работе с обращениями граждан, содержащими информацию о преступлении или об административном правонарушении……. 16

Копцов С.В. Особенности рассмотрения отдельных категорий обращений граждан……... 22

Ларина А.Ю. Анализ контроля за исполнением поручений руководителя……. 28

Разиньков А.С., Куликов А.С. Методы предупреждения распространения идеологии «скулшутинга» с использованием сети Интернет……... 30

Власенко А.В. Инновационные технологии в делопроизводстве органов внутренних дел: применение блокчейн-технологий для обеспечения прозрачности и безопасности …… 35

Куминов М.В. Электронный документооборот с использованием сервиса электронной почты: преимущества и недостатки …… 41

Датиев А.А., Горзолия М.В. Роль подразделения делопроизводства в обеспечении защищенного документооборота в органах внутренних дел……..... 46

Датиев А.А., Дзагкоев С.Р. Программно-аппаратная защита в делопроизводстве……... 49

Назаров А.К. Криптография: современные алгоритмы и ее будущее…… 52

Еськов Александр Васильевич,
доктор технических наук, профессор

ПРИМЕНЕНИЕ МЕТОДА ЭКСПЕРТНЫХ ОЦЕНОК ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ СОТРУДНИКАМИ ОТДЕЛА ДЕЛОПРОИЗВОДСТВА И РЕЖИМА

При оценке объектов исследования эксперты зачастую расходятся во мнениях по решаемой проблеме. В связи с этим возникает необходимость количественной оценки степени согласия экспертов. Получение количественной меры согласованности позволяет более обоснованно интерпретировать причины расхождения мнений.

При использовании количественных шкал измерения и оценке всего одного объекта все мнения экспертов можно представить, как точки на числовой оси. Эти точки можно рассматривать как реализации случайной величины и поэтому для оценки центра группировки и разброса точек представляется возможным использовать хорошо разработанные методы математической статистики. Центр группировки точек можно определить, как математическое ожидание (среднее значение) или медиану случайной величины, разброс количественно оценивается дисперсией случайной величины. Мерой согласованности оценок экспертов, т.е. компактности расположения точек на числовой оси, может служить отношение среднеквадратического отклонения к математическому ожиданию случайной величины.

При измерении объектов в порядковой шкале согласованность оценок экспертов в виде ранжировок или парных сравнений объектов также основывается на понятии компактности.

Метод простого ранжирования заключается в том, что каждый эксперт располагает признаки в порядке предпочтения. Цифрой 1 обозначается наиболее важный признак, цифрой 2 - следующий по важности и т. д. Полученные результаты сводятся в таблицу, общий вид которой представлен в таблице 1.

Таблица 1. Сводная таблица результатов

Признаки или объект оценки	Эксперты					
	1	2	3	4	s	d
X_1	r_{11}	r_{12}	r_{13}	r_{14}	r_{1s}	r_{1d}
X_2	r_{21}	r_{22}	r_{23}	r_{24}	r_{2s}	r_{2d}
X_3	r_{31}	r_{32}	r_{33}	r_{34}	r_{3s}	r_{3d}
X_i	r_{i1}	r_{i2}	r_{i3}	r_{i4}	r_{is}	r_{id}
X_m	r_{m1}	r_{m2}	r_{m3}	r_{m4}	r_{ms}	r_{md}

Рассмотрим матрицу (табл. 1) результатов ранжировки m объектов группой из d экспертов $\|r_{is}\|$, $S = \overline{(1,d)}$, $i = \overline{(1,m)}$, где r_{is} - ранг, присваиваемый s-экспертом i-му объекту.

Составим суммы рангов по каждой строке. В результате получим вектор с компонентами $r_i = \sum_{s=1}^{d} r_{is}$ $i = \overline{1,m}$.

Будем рассматривать величины r_i как реализации случайной величины и найдем оценку дисперсии. Как известно, оптимальная по критерию минимума среднего квадрата ошибки оценка дисперсии определяется формулой:

$D = \frac{1}{m-1}\sum_{i=1}^{m}(r_i - \bar{r})^2$, где $\bar{r} = \frac{1}{m}\sum_{i=1}^{m} r_i$ - оценка математического ожидания.

Коэффициент степени согласованности мнений экспертов (коэффициент конкордации) рассчитывается по формуле:

$$\mathrm{W} = \frac{12\mathrm{D}}{(\mathrm{m}^2-1)},$$

Данная формула определяет коэффициент конкордации для случая отсутствия связных рангов.

При W=0 согласованность оценок различных экспертов отсутствует, а при W=1 согласованность мнений экспертов полная.

При крайних коэффициентах конкордации могут быть даны следующие рекомендации.

Если W=0, то для получения достоверных оценок следует уточнить исходные данные о событиях и (либо) изменить состав группы экспертов.

При W=1 не всегда можно считать оценки объективными, поскольку может оказаться, что все члены экспертной группы условились придерживаться одинаковых взглядов.

Необходимо, чтобы найденное значение W было больше заданного значения. Обычно принимается W=0,5, т.е. при W>0,5 выводы экспертов согласованы в большей мере, чем несогласованы. При W<0,5 оценки нельзя считать в достаточной степени согласованными.

Возможно нахождение эксперта с мнением, отличающимся от других. Для этого нужно рассчитать W для группы экспертов без эксперта с отличающимся мнением. Например, убрать из расчета 3 столбец!

Если W с участием этого эксперта меньше, чем без его участия в расчетах, то это и укажет на его позицию, отличную от остальных экспертов.

Фрагмент расчета согласованности мнений экспертов по вопросам анкеты приведен в таблице 2.

Таблица 2. Согласованность мнений экспертов

		Эксперты							
№	Вопрос	1, 2, 3	4, 5	6, 7, 8	9, 10	11, 12	13, 14	15, 16, 17	18, 19
1	Не написан акт квартальной проверки за 2 квартал	2	3	2	4	5	6	8	1
2	У начальника находятся секретные документы, переданные ему на доклад без подписи	1	5	5	11	11	10	4	2
3	В помещении РСП хранятся конверты от корреспонденции, полученной 2 недели назад.	16	6	15	16	18	16	7	6
4	На окнах помещения РСП отсутствуют решетки (I этаж)	12	16	13	2	10	3	9	15
5	В сейфе лежат два мешка секретных документов, числящихся уничтоженными	3	2	14	1	6	4	2	3
6	В отделе закончился чай (кофе)	18	18	18	18	17	18	18	18
7	В двух карточках формы 1, вернувшихся 2 дня назад из органа безопасности, отсутствуют отметки руководителя о допуске (переоформление)	6	12	6	10	2	7	14	13
8	Срок рассмотрения 2 обращений граждан истекает через 3 дня (исполнитель - Вы, одно из них уже продлевалось)	14	4	16	14	3	14	16	16
9	На вашем объекте информатизации подключена клавиатура, не входящая в состав комплекта (родная неисправна)	13	15	11	3	7	15	6	14
10	После смены замков в двух режимных помещениях вам не сдали вторые экземпляры ключей	9	13	9	8	12	13	12	4
11	Начальник отдела Иванов И.И. утром спрашивал, не встречался среди других документов секретный рапорт о проведении мероприятия	15	1	1	12	16	2	1	5
12	Не проставлены отметки в карточках учета осведомленности 15 сотрудников, вернувшихся на этой неделе из командировки	5	7	10	15	13	9	15	11
13	Охранная сигнализация выделенного помещения вышла из строя.	11	11	12	13	8	5	10	10
14	Еще утром у Вас поднялась температура	17	17	17	17	14	17	17	17
15	Заместитель начальника отдела Петров П.П. убыл в отпуск, не отчитавшись за числящиеся за ним документы	4	8	7	5	15	1	5	7
16	По итогам годовой проверки часть записей осталась не заверенной штампом «Учет сверен»	7	9	3	6	4	11	3	8
17	Некоторые сотрудники имеют дополнительные экземпляры ключей от входных дверей кабинетов и сейфов в результате чего иногда забывают делать отметки о вскрытии в дежурной части	9	14	8	7	9	12	11	9
18	В журнале регистрации подготовленных секретных документов имеются «забронированные номера» еще с прошлого месяца	8	10	4	9	1	8	13	13

На слайде для примера расчета приведены 15 ситуационных вопросов и мнения 8 экспертов (группы из слушателей, имеющих стаж работы в подразделениях ОДИР до 3 лет). Видно, что каждая группа по-разному ранжирует каждый вопрос.

Например, на 3 вопрос эксперты 4,5, 15, 16, 17 , 18 и 19 групп поставили ранг 6-7, в то же время, остальные эксперты групп 1, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14 установили ранг 16 – 18. На лицо значительное расхождение во мнениях указанных экспертов.

В то же время, коэффициенты согласованности (конкордации) мнений экспертов:

для 1 группы экспертов (18 человек) W=0,44;

для 2 группы экспертов (8) W=0,49;

для 3 группы экспертов (2) W=0,91;

для 4 группы экспертов (контрольная) W=0,81.

Для укрупненной группы экспертов из числа сотрудников ОДИР, имеющих стаж работы до 3 лет, W=0,91, в то время как для контрольной группы экспертов из числа сотрудников ОДИР, имеющих стаж работы более 3 лет на должностях руководителей отделов, W=0,81.

Распределение вопросов по рангам для 19 экспертов приведено в виде диаграммы на рисунке 1.

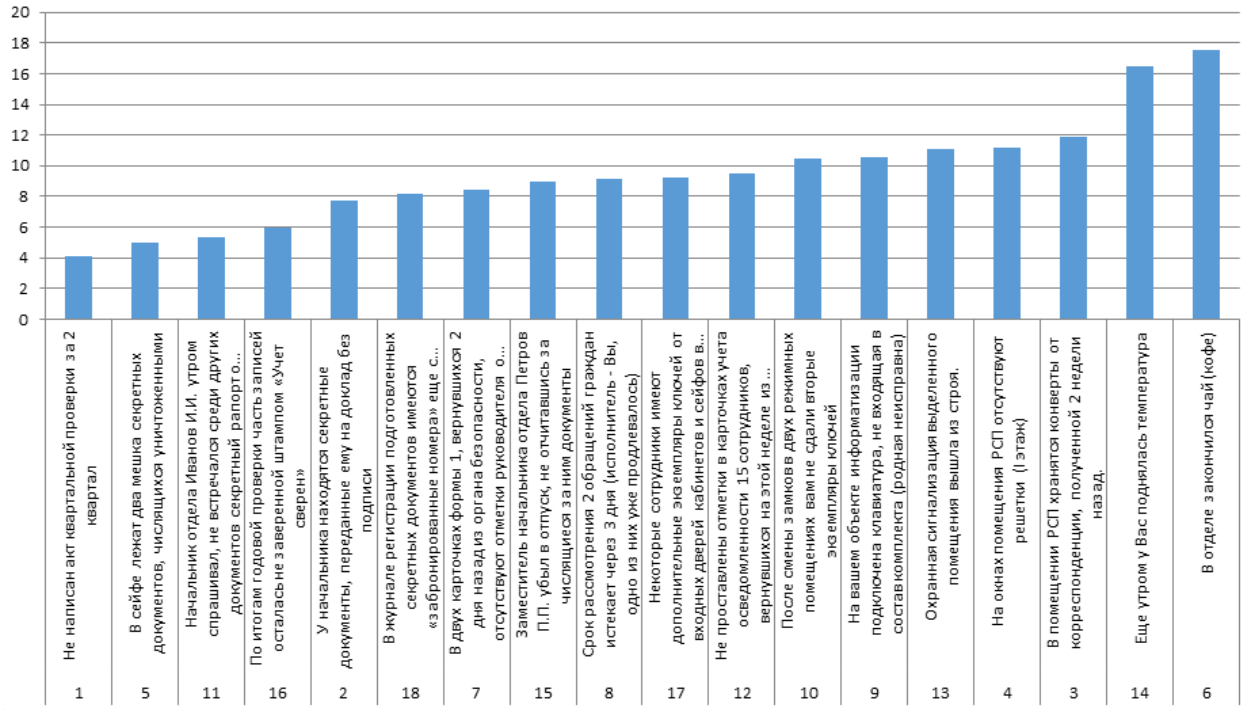


Рис.1. Распределение вопросов по рангам для 19 экспертов

Из диаграммы видно, сколько экспертов поставили одинаковый ранг тому или иному вопросу.

На рисунке 2 приведено распределение вопросов по рангам для 2 экспертов (групп).

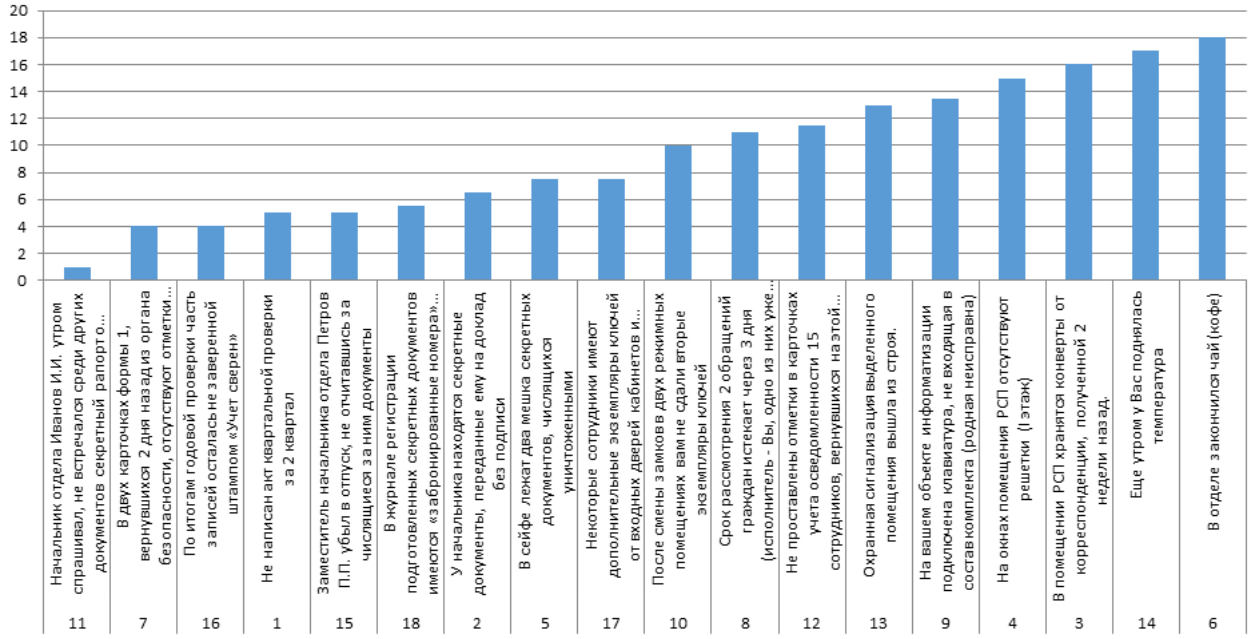


Рис.2. Распределение вопросов по рангам для 2 экспертов

Из 1 и 2 диаграмм видно, что вопрос под номером 11 переместился на 1 место по рангу для укрупненных групп экспертов, то есть для двух экспертов.

На 3 рисунке приведено распределение вопросов для контрольной группы экспертов.

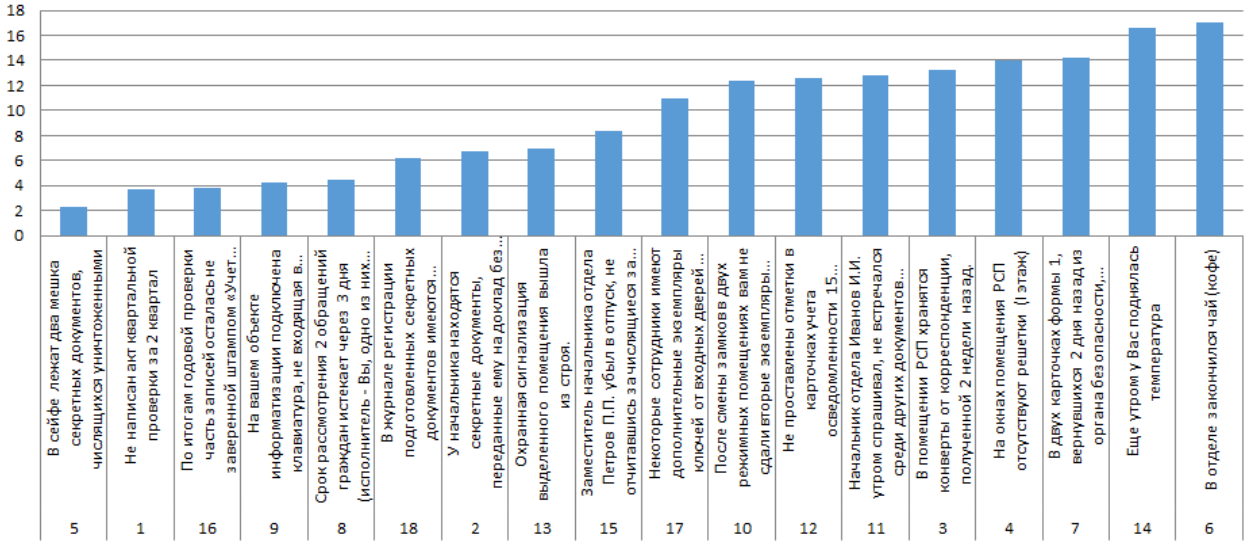


Рис.3. Распределение вопросов распределение вопросов для контрольной группы экспертов

Из диаграммы видно, что вопрос под номером 11 имеет 13 ранг и не относится к наиболее важным по мнению экспертов контрольной группы. Первое место занял вопрос, который эксперты двух групп (рис.2) определяли только на 8 место.

Проведенные исследования приводят к следующим выводам:

метод экспертных оценок позволяет количественно определить ранг вопроса (уровень важности ситуации) на основе мнений более опытных коллег;

метод экспертных оценок позволяет определить сотрудника, мнение которого отличается от большинства более согласованных мнений;

значение коэффициента согласованности мнений экспертов близкое к единице не гарантирует правильность ранжирования ситуационных вопросов;

применение метода экспертных оценок при проведении занятий в форме деловой игры позволяет обучаемым с небольшим опытом работы убедиться в правильном выборе ранга ситуационного вопроса на основе мнений большинства и контрольной группы экспертов.

Звонарева Анна Юрьевна,
кандидат социологических наук,
начальник кафедры организации
деятельности органов внутренних дел
центра командно-штабных учений
Академии управления МВД России

О ПРОБЛЕМНЫХ ВОПРОСАХ КООРДИНАЦИИ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ, ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ И РАССМОТРЕНИЯ ОБРАЩЕНИЙ

Приказом МВД России от 23 декабря 2020 г. № 888[1] [6] было утверждено «Типовое положение о подразделении делопроизводства и режима территориального органа МВД России». Согласно пункту 9.4 данного положения, основной задачей подразделений делопроизводства и режима[2] выступает координационная деятельность ТО МВД России, а также структурных и подчиненных подразделений по вопросам обеспечения защиты государственной тайны, документационного обеспечения управления и рассмотрения обращений, контроль за выполнением требований законодательных и иных нормативных правовых актов в соответствующих сферах деятельности.

Термин «координация» упоминается в названном источнике только один раз без толкования его содержания.

Поэтому для точного уяснения указанной правовой категории, а соответственно и задачи ПДиР, обратимся к толковому словарю русского языка. Так, С.И. Ожегов и Н.Ю. Шведова в своем труде отмечают, что «Координировать, то есть согласовать (-вывать) или же установить (-навливать) целесообразное соотношение между какими-нибудь действиями, явлениями» [8].

Согласно теории управления, термин «координация» появился в начале XX века, впервые его ввел французский горный инженер Анри Файоль, использовав в своей работе «Общее и промышленное управление». Стоит отметить, что последователи ранней классической индустриальной парадигмы, в ходе которой и стали упоминать данное определение, считали «управляемую организацию за механический обезличенный агрегат из индивидов, все отношения между которыми поддаются рационализации» [1, 7].

Рационализировать означает «совершенствуя организовывать что-либо более рационально, то есть разумно обоснованно и целесообразно» [8].

---

[1] Далее – также «приказ».

[2] Далее – также «ПДиР».

Под координацией Анри Файоль понимал свободный обмен информацией и «открытость» в деятельности служб и ее структурных подразделений, однако другие исследователи в рамках классической теории управления в 1940-1960 гг. подвергли критическому анализу в связи с появлением иных управленческих концепций.

Естественно, что сотню лет назад ни о каком подробном изучении «координации деятельности» по вопросам обеспечения защиты государственной тайны, документационного обеспечения управления и рассмотрения обращений не могло быть и речи.

Отметим, что в рамках ведомственных научных трудов в настоящее время затрагиваются лишь некоторые аспекты указанной тематики. Вместе с тем как никогда актуально осветить существующие проблемы в рассматриваемой области комплексно.

Так, проблемные вопросы координационной деятельности в области обеспечения защиты государственной тайны, документационного обеспечения управления и рассмотрения обращений схожи и с проблемами рациональности, которые являются классическими для теории управления [1, 2, 3, 4, 5, 7].

Немецкий социолог Макс Вебер, который являлся одним из основателей концепции рациональности, определял «рациональность» как целесообразность и связывал ее с эффективностью, под которой понимал достижение результата с наименьшими затратами [2]. Он подразделял на две категории: позитивную и негативную. Так, по его мнению, позитивная рациональность, выступает в роли количественного учета всех операций и действий, в то время как негативная рациональность – это рациональность сама по себе, она может быть взята как самоцель, которая будет оторвана от предпочтений людей.

По мнению Макса Вебера, примером рациональности является бюрократия. Позитивная бюрократия экономит ресурсы, время и обеспечивает качественную работу, а вот негативная, напротив, создает избыток ненужных документов и занимается бессмысленной бумажной волокитой.

С учетом этого подхода при эффективной координации в сфере защиты государственной тайны, документационного обеспечения управления и рассмотрения обращений должна существенно уменьшаться документационная нагрузка на личный состав.

О существующих проблемах снижения документационной нагрузки личного состава в органах внутренних дел хорошо известно – их наличие ежегодно анализируется в связи с проведением работы по оптимизации документооборота.

Вместе с тем, как отмечают в ОАД МВД России, меры, предпринимаемые с начала 2010-х годов и по настоящее время в указанной сфере деятельности, хотя и приносят определенный результат, но их действие носит временный (цикличный) характер. Как правило, улучшение наступает после

проведения целевого мероприятия и (или) издания очередного управленческого решения и длится определенный период. Затем, по ряду причин объективного (изменение условий функционирования) и субъективного (устоявшиеся традиции на фоне текучести кадров) характера, ситуация становится прежней или ухудшается.

Любой территориальный орган МВД России является сложной социальной системой. Успешное решение предусмотренной приказом задачи ПДиР возможно лишь при формировании в ТО МВД России такой организационной культуры, которая была бы направленна на укрепление духа корпоративности и осознания единства целей в рассматриваемой области. То есть порядок действий и сами действия всех должностных лиц могли бы быть прогнозируемы в этой общей для всех «системе координат» для «установления целесообразного соотношения между действиями» структурных и подчиненных подразделений ТО МВД России.

Среди широко распространенных проблем, которые не позволяют обеспечить необходимую для снижения нагрузки согласованность действий в рассматриваемой сфере, можно выделить следующие:

1. Устойчивая тенденция роста объемов документопотоков в органах внутренних дел.

2. Несоответствие отчетных сведений действительному положению дел в сфере обеспечения защиты государственной тайны, документационного обеспечения управления, а также рассмотрения обращений.

3. Несовершенная для исключения имеющихся вопросов координации управленческая, организационная и штабная культура в территориальных органах МВД России.

Без сомнения, основным параметром результативности управления является достижение ожидаемого исхода в преобразовании предмета воздействия. Координацию можно интерпретировать не как отдельно существующую операцию, а рассматривать в тесной связи со всеми управленческими функциями контроля (информационной, аналитической, прогнозирования, планирования, организации, регулирования).

Кроме того, координация, а значит и рациональность совместных действий, не должна быть самоцелью при выполнении задачи ПДиР. Иначе такой подход может приводить к заорганизованности действий должностных лиц, что является крайне нежелательным явлением в условиях постоянного изменения оперативной обстановки.

В связи с изложенным сделаем несколько выводов:

1. Проблемные вопросы координационной деятельности в сфере обеспечения защиты государственной тайны, документационного обеспечения управления, а также рассмотрения обращений схожи с проблемами рациональности, которые традиционны для теории управления, и связаны с устойчивой тенденцией роста объемов документопотоков в органах внут-

ренних дел; несоответствием отчетных сведений действительному положению дел в указанных сферах; недостаточной управленческой, организационной и штабной культурой в ТО МВД России.

2. Координационную деятельность территориальных органов МВД России и их структурных и подчиненных подразделений по вопросам обеспечения защиты государственной тайны, документационного обеспечения управления, а также рассмотрения обращений целесообразнее рассматривать в неразрывной связи со всеми управленческими функциями (информационной, аналитической, прогнозирования, планирования, организации, регулирования, контроля), а значит успешное решение задачи ПДиР зависит от принимаемых заинтересованными руководителями управленческих решений.

Литература

1. Веселый В.З. Формирование теории управления в сфере правоохранительной деятельности и совершенствование управленческой подготовки кадров в органах внутренних дел: дис. ... докт. юрид. наук: 12.00.11 / Весёлый Валериан Зямович. - М., 1988. - 286 с.

2. Звонарева А.Ю. Документационное обеспечение управления в органах внутренних дел Российской Федерации: проблемы и перспективы развития // Труды Академии управления МВД России. 2020. № 1 (53). С. 40-47.

3. Зинуров Р.Н. Концептуальные основы и научно-практические проблемы координации деятельности правоохранительных органов в борьбе с преступностью (тенденции и закономерности): дис. ... докт. юрид. наук: 12.00.11 / Зинуров Рафаил Наримановичь. Уфа. 2003. - 351 с.

4. Иващук А.В. Межрегиональная координация правоохранительной деятельности территориальных органов МВД России: дис. ... канд. юрид. наук: 12.00.11 /Иващук Александра Владимировна. М., 2018. - 220 с.

5. Майдыков А.Ф. Совершенствование управления городскими и районными органами внутренних дел (теоретические и организационно - правовые основы): дис. д-ра юрид. наук: 12.00.11 / Майдыков Анатолий Федорович. М., 1985. - 428 с

6. Приказ МВД России от 23 декабря 2020 г. № 888 «Об утверждении Типового положения о подразделении делопроизводства и режима территоиального органа МВД России» [Электронный ресурс] – Режим доступа свободный: СПС «Консультант Плюс» (дата обращения: 14.10.2024).

7. Теория управления в сфере правоохранительной деятельности: учебник для слушателей Академии МВД СССР / В.З. Весёлый, Г.М. Воскресенский [и др.]: под ред. докт-ра. юрид. наук, профессора В.Д. Малькова. – М., Академия МВД СССР, 1990. – 324 с.

8. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / С.И. Ожогов, Н.Ю, Шведова; Российская академия наук. Институт русского языка им. В.В. Винградова. – 7-е изд., дополненное. – М.: Азбуковник, 1999. – 944 с.

Федченко Андрей Дмитриевич,
начальник отдела ОДиР УБК МВД России

АКТУАЛЬНЫЕ ВОПРОСЫ ЦИФРОВИЗАЦИИ ДОКУМЕНТАЦИОННОГО ОБЕСПЕЧЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Указом Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» цифровая трансформация государственного и муниципального управления, экономики и социальной сферы определена одной из национальных целей.

Подразделения МВД России активно участвуют в данном направлении деятельности. На постоянной основе создаются и модернизируются всевозможные цифровые сервисы и ресурсы, значительным образом влияющие на скорость прохождения информации и результативность мероприятий, проводимых органами внутренних дел.

Однако, на практике, мы зачастую сталкиваемся с проблемами, вызванными несовершенством действующей нормативной правовой базы, сложностями, связанными с разработкой и внедрением программных продуктов, а также недостатками, возникающими в результате ненадлежащего использования уже существующих систем.

Приведенные в докладе Алевтины Владимировны примеры работы с обращениями граждан, содержащими признаки преступления, ярко демонстрируют актуальность вышеуказанной проблематики.

Если для Севастополя срок прохождения обращения до исполнителя составляет 10-15 дней, то для подразделений Центрального аппарата МВД России эти цифры составляют от 10 до 30 дней и регистрация примерно в 15 формах, после чего в силу специфики раскрываемых преступлений так называемые заявления начинают свое турне по стране.

Один из приведенных ею примеров я бы хотел разобрать с точки зрения организации так называемого юридически значимого документооборота.

Как уже было сказано ранее, частью первой статьи 4742 уголовно процессуального кодекса установлен прямой запрет направления заявления о преступлении в форме электронного документа.

Наряду с этим, пунктами 10, 11, 12 Инструкции о порядке приема заявлений и сообщений о преступлениях, утвержденной приказом МВД России от 29 августа 2014 г. № 736 предусмотрено, что для приема заявлений о преступлениях в электронной форме, направляемых посредством официальных сайтов, применяется специальное программное обеспечение.

Такие заявления распечатываются на бумажном носителе, и по непонятным основаниям дальнейшая работа ведется с ними как с письменными заявлениями о преступлениях.

Вместе с тем, обращения, поступившие в бумажном виде, сперва сканируются, в электронном виде докладываются руководителю, а затем распечатывается в дежурной части, после чего опять сканируется и опять распечатывается.

В результате вышеуказанных манипуляций, на мой взгляд, юридическая значимость заявления, направленного в органы внутренних дел в письменном виде утрачивается.

Существует мнение, что предоставление гражданам Российской Федерации права направлять заявления и сообщения о преступлении в электронной форме может значительным образом увеличить их количество и как следствие нагрузку на органы внутренних дел.

Я эту точку зрения не разделяю, и считаю, что разработка и внедрение в эксплуатацию программного обеспечения, позволяющего гражданам подать заявление в электронном виде непосредственно в ближайший территориальный орган снизит излишний документооборот, нагрузку на личный состав и повысит эффективность принимаемых мер реагирования.

Теперь давайте попробую обосновать свою точку зрения и объяснить какие инструменты цифровизации могут помочь нам стать лучше.

В соответствии с частью 1 статьи 6 Федерального закона Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Таким образом, документ, составленный в электронной форме и подписанный электронной подписью, является равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Кроме того, часть 3 этого же закона гласит, что если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

На сегодняшний день в системе органов внутренних дел уже осуществляется юридически значимый документооборот по различным направлениям деятельности, таким как:

– служебная переписка направляемая и получаемая посредством межведомственной системы электронного документооборота (т.н. МЭДО);

– информационное взаимодействие с налоговой службой по финансовым вопросам;

– информационное и документационное взаимодействие в рамках оказания государственных услуг и по линии ГИБДД;

– ответы, направляемые гражданам в рамках работы с обращениями граждан и организаций.

Возможно существуют и другие системы о которых я не вспомнил или не знаю. Однако, наряду с вышеизложенными системами существуют и иные, не относящиеся к понятию «юридически значимого документооборота». Это так называемый канал «пришлите мне на электронную почту». В чем здесь нюанс?

Юридически значимым может быть признан электронный документ подписанный цифровой подписью. Бытует мнение, что pdf-файл с картинкой «подписано цифровой подписью» является тем самым электронным документом, но это либо не совсем так, либо совсем не так.

Я сейчас не буду подробно останавливаться на вариантах и расширениях откреплённых и прикреплённых цифровых подписей и различных трактовках самого термина, однако скажу, что система электронного документооборота ИСОД МВД России на сегодняшний день не позволяет исполнителю самостоятельно каким-либо способом скачать подготовленный электронный документ себе на компьютер.

В связи с этим, достаточно удобный механизм согласования и подписания документов, подготовленных в электронной форме, на мой взгляд не до конца доработан и не позволяет осуществлять «юридически значимый» документооборот с организациями, не подключенными к системе МЭДО, но использующими аналогичные системы электронного документооборота.

Что, например, является актуальным при взаимодействии с операторами связи, организаторами распространения информации, коммерческими и банковскими структурами.

Кроме того, данное положение дел существенным образом тормозит развитие систем, используемых в оперативных и следственных интересах.

Так, например, широкое распространение машиночитаемых документов и алгоритмов API в наших системах позволит постепенно приблизится к появлению сервисов, работающих по принципу «единого окна», когда уполномоченный сотрудник сможет получать максимальное количество информации при совершении минимального количества действий.

Уже давно существует система межведомственного электронного взаимодействия (т.н. СМЭВ) развернутая с использованием защищенных каналов связи. Данная система позволяет осуществлять оперативный обмен достоверными сведениями из различных баз данных.

В завершение своего доклада хочу сказать, что при всей кажущейся сложности поставленных перед нами задач, благодаря совместным усилиям мы сможем их решить. Поэтому призываю не останавливаться на достигнутом и активнее объединяться, делиться мыслями, идеями и положительным опытом.

Черкашина Алевтина Владимировна,
начальник отделения по работе
с обращениями граждан и организаций
Отдела делопроизводства и режима
УМВД России по г. Севастополю

ПРОБЛЕМНЫЕ ВОПРОСЫ В РАБОТЕ С ОБРАЩЕНИЯМИ ГРАЖДАН, СОДЕРЖАЩИМИ ИНФОРМАЦИЮ О ПРЕСТУПЛЕНИИ ИЛИ ОБ АДМИНИСТРАТИВНОМ ПРАВОНАРУШЕНИИ

Одним из направлений ОДиР является работа по совершенствованию российского законодательства в сфере формирования нормативно-правовой основы регулирования обращений граждан в форме электронного документа.

Данное направление представляет особый интерес в условиях цифровизации уголовного процесса, который должен брать свое начало именно с этапа рассмотрения сообщения о преступлении. В настоящий момент существует необходимость автоматизации процесса подачи и регистрации сообщения о преступлении, которая включала бы в себя также предупреждение об уголовной ответственности за заведомо ложный донос. Цифровизация этапа рассмотрения сообщения о преступлении, поможет снизить количество нарушений прав граждан при приеме, регистрации и рассмотрении заявлений о преступлении, повысить результативность и оперативность расследования.

Наряду с этим существующая практика подачи и рассмотрения в органах внутренних дел обращений и заявлений граждан, а также нормативная база, регламентирующая данную деятельность, не отвечает современным запросам общества, имеет ряд недостатков, значительным образом увеличивает документооборот, требует привлечения значительных временных и человеческих ресурсов.

На сегодняшний день сложилась ситуация, при которой граждане не имеют возможности подать заявление о преступлении в электронном виде, а существующее программное обеспечение Сервиса работы с обращениями граждан не содержит всех необходимых реквизитов для работы с заявлениями о преступлении или правонарушении.

1. Обращения граждан, поступившие о органы внутренних дел в электронной форме и содержащие информацию о преступлениях, об административных правонарушениях требуют оперативного принятия конкретных мер реагирования. Однако, в связи с установленным графиком работы подразделений делопроизводства и режима, а также сроками и алгорит-

мами, предусмотренными для работы с обращениями граждан, своевременная реализация указанных мер реагирования не представляется возможной. **Например:** На основании части 2 статьи 8 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» регистрация обращений граждан и организаций производится в течение трех дней с момента поступления.

Согласно пункту 125 Инструкции по делопроизводству в органах внутренних дел Российской Федерации, утвержденной приказом МВД России от 2 сентября 2024 г. № 515, подразделения делопроизводства и режима осуществляют прием корреспонденции, поступающей в орган внутренних дел в рабочее время.

Таким образом обращения граждан и организаций, в том числе содержащие информацию о готовящихся или совершенных преступлениях, поступившие в подразделение в пятницу, будут зарегистрированы не раньше понедельника, а поступившие накануне новогодних или майских праздников, в первый рабочий день по их окончанию.

Обращения граждан, в которых сообщается о преступлениях (правонарушениях), поступившие посредством операторов связи или официальных сайтов в установленном порядке проходят регистрацию в качестве обращения. Затем, согласно резолюции руководителя УМВД, эти заявления направляются в ДЧ. Дежурная часть регистрирует заявление в КУСП, в СОДЧ, и готовит к нему сопроводительное письмо для пересылки на исполнение в подчиненный территориальный орган либо подразделение. Сопроводительное письмо о передаче материала КУСП передается на регистрацию в ОДиР, сотрудниками которого вносятся необходимые сведения в СЭД ИСОД и, соответственно присваивается исходящий регистрационный номер, после чего документы в бумажном виде направляются адресату (в электронном виде документ сразу же поступает по СЭД в ОМВД).

Далее указанный материал КУСП проходит аналогичную регистрацию в подчиненном территориальном органе или подразделении.

После регистрации поступившего материала в журнале КУСП и СОДЧ материал, наконец-то передается на исполнение сотруднику.

При такой схеме срок прохождения документа с момента поступления в подразделение делопроизводства и режима до получения материала исполнителем занимает от 5 до 15 дней, в течение которых само обращение и сопутствующие материалы проходят регистрацию примерно в 7 учетных формах, и в указанный период, в большинстве случаев, никаких конкретных мероприятий по обращению, содержащему информацию о преступлении, не проводится, процессуальные сроки постоянно обновляются.

Кроме этого, о каждой регистрации в КУСП, а затем о результатах рассмотрения и принятом решении должен быть проинформирован гражданин, направивший заявление, что приводит к постоянному направлению

«пустых писем», недовольству граждан и как следствие повторным обращениям и жалобам.

В части 1 статьи 12 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» указано, что на полицию возлагаются обязанности принимать и регистрировать (в том числе в электронной форме) заявления и сообщения о преступлениях.

Пунктом 9 Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, утвержденной приказом МВД России от 29 августа 2014 г. № 736[1] предусмотрено, что круглосуточный прием заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях осуществляется оперативным дежурным дежурной части территориального органа МВД России (управления, отдела, отделения, пункта полиции, линейного отдела, линейного отделения, линейного пункта полиции).

Для этих целей пунктом 10 Инструкции о порядке приема заявлений и сообщений о преступлениях, предусмотрено применение программного обеспечения, предусматривающего обязательное заполнение заявителем реквизитов, необходимых для работы с заявлениями о преступлениях, об административных правонарушениях, о происшествиях.

Отсутствие на сегодняшний день соответствующего программного обеспечения в МВД России вынуждает граждан направлять «заявления о преступлениях» через существующий сервис «Прием обращений граждан и организаций» аппаратно-программного комплекса «Официальный интернет-сайт МВД России» (далее – Сервис), который создан исключительно для подачи обращений граждан и организаций в целях реализации положений Федерального закона от 2 мая 2006 г. № 59-ФЗ «О рассмотрении обращений граждан Российской Федерации» (далее – Федеральный закон № 59-ФЗ).

Программное обеспечение Сервиса предусматривает обязательное указание гражданином исключительно сведений, определенных статьей 7 Федерального закона № 59-ФЗ (фамилия, имя, отчество (при наличии) заявителя; адрес электронной почты; суть предложения, заявления или жалобы), и не содержит всех необходимых реквизитов для работы с заявлениями о преступлении, при этом идентификация и аутентификация авторов обращений законодательством не предусмотрена.

В этой связи у подразделений, рассматривающих заявления о преступлении, поступившие посредством Сервиса в подразделения делопроизводства и режима (далее – ПДиР), возникает множество проблем при их разрешении (идентификация автора обращения, определение места события,

---

[1] Далее – «Инструкции о порядке приема заявлений и сообщений о преступлениях».

уточнения у автора обращения сведений необходимых для принятия решения о наличии состава преступления, при принятии решения о признании таких обращений анонимными).

Таким образом отсутствие специального программного обеспечения крайне негативно влияет на оперативность реагирования органов внутренних дел на сообщения о преступлениях и правонарушениях.

Хочу обратить Ваше внимание, что в соответствии с частью первой статьи 474.2 Уголовно-процессуального кодекса Российской Федерации ходатайство, заявление, за исключением заявления о преступлении, при наличии технической возможности могут быть поданы в форме электронного документа и подписываются лицом, подавшим такой документ усиленной квалифицированной электронной подписью.

Согласно части первой статьи 141 УПК РФ заявление о преступлении может быть сделано в устном и письменном виде.

Таким образом, УПК РФ установлен прямой запрет направления заявления о преступлении в форме электронного документа.

Пунктом 12 Инструкции о порядке приема заявлений и сообщений о преступлениях, предусмотрено, что заявления о преступлениях, об административных правонарушениях, содержащиеся в письменных обращениях заявителей, направленных посредством официальных сайтов, принимаются подразделением делопроизводства и режима территориального органа МВД России регистрируются в установленном порядке и направляются руководителем (начальником) территориального органа МВД России в дежурную часть для незамедлительной регистрации в КУСП.

Данная норма противоречит положениям УПК РФ другим нормативным правовым актам, регулирующим порядок приема и регистрации заявлений и сообщений о преступлениях по нескольким причинам:

1. Заявление и сообщение о преступлении не может быть подано посредством официального сайта МВД России, так как их электронная форма действующими нормативными правовыми актами не предусмотрена.

2. Степень юридической подготовки сотрудников ПДиР в большинстве случаев не позволяет им обнаруживать в обращениях состав преступлений.

3. Сотрудники ПДиР не уполномочены на регистрацию заявлений и сообщений о преступлении.

Принимая во внимание, изложенное также требуют корректировки пункты 69 и 70 Инструкции 707 в части направления и приема обращений граждан на регистрацию в КУСП.

Справочно: пункт 69. Обращение, содержащее информацию о преступлении или об административном правонарушении, поступившее в подразделение делопроизводства в соответствии с пунктом 27 Инструкции, регистрируется, учитывается, докладывается руководителю территориаль-

ного органа и с его поручением передается в дежурную часть для регистрации в КУСП незамедлительно. Сотрудник подразделения делопроизводства в установленном порядке сообщает гражданину о дате и номере регистрации его обращения в КУСП и вносит указанные сведения в учетные формы подразделения делопроизводства.

Пункт 70. Обращение, содержащее информацию о преступлении, об административном правонарушении, поступившее в Министерство или его структурное подразделение, регистрируется и учитывается в порядке, установленном Инструкцией, после чего направляется в территориальный орган на межрегиональном или региональном уровне для регистрации в КУСП.)

В соответствии с пунктом 12 Инструкции о порядке приема заявлений и сообщений о преступлениях заявления о преступлениях, об административных правонарушениях, о происшествиях, содержащиеся в письменных обращениях заявителей, направленных посредством операторов почтовой связи с доставкой письменной корреспонденции в здание территориального органа МВД России, федеральной фельдъегерской связи и специальной связи, почтового ящика, полученных в ходе личного приема, принимаются подразделением делопроизводства и режима территориального органа МВД России, регистрируются в установленном порядке и направляются руководителем (начальником) территориального органа МВД России в дежурную часть для незамедлительной регистрации в КУСП.

Следует отметить, что на сегодняшний день в подразделениях МВД России применяется электронная форма регистрации и дальнейшей работы с обращениями. Таким образом все обращения, поступившие на бумажных носителях, сканируются.

В соответствии с пунктом 11 указанной Инструкции электронные заявления распечатываются на бумажном носителе, дальнейшая работа ведется с ними как с письменными заявлениями о преступлениях, об административных правонарушениях, о происшествиях.

Таким образом возникает ситуация, при которой обращение, поступившее на бумажном носителе, сперва сканируется, в электронном виде докладывается руководителю, а затем распечатывается в дежурной части. Причем срок между сканированием и распечатыванием одного и того же документа может составлять менее часа. После принятия решения о передаче данного обращения по территориальности в большинстве случаев данный документ опять сканируется (только уже как подготовленный документ) и распечатывается адресатом. Данная схема с одним и тем же документом может повторяться несколько раз.

В целях ускорения процесса прохождения заявлений о преступлении, экономии бумаги и времени, целесообразно внести изменения в вышеуказанную норму и поручить ПДиР передавать заявления о преступлениях, поступившие на бумажных носителях, напрямую в дежурную часть территориального органа.

Учитывая, что в последующем материалы по рассмотрению заявления (сообщения) о преступлении пересылаются через общую канцелярию, представляется целесообразным указанные заявления регистрировать в журнале учета пакетов или в разделе поступивших документов СЭД ИСОД МВД России.

В своей статье «Особенности использования электронных документов на этапе рассмотрения сообщения о преступлении», адъюнкт факультета подготовки научно-педагогических и научных кадров Московского университета Министерства внутренних дел Российской Федерации имени В.Я. Кикотя Демичева Татьяна Сергеевна пишет, что «при рассмотрении существующих вопросов в уголовно-процессуальном законодательстве относительно использования электронных документов на начальной стадии уголовного производства, можно предложить такие пути решения обозначенных проблем, как законодательное закрепление в ст. 141 УПК РФ возможности подачи заявления о преступлении в форме электронного документа. Это потребует создания алгоритма получения и регистрации сообщения о преступлении, а также создания единой платформы, позволяющей гражданам обратиться с заявлением о преступлении.

Подводя итог сказанному можно сделать вывод, что на сегодняшний день работа с заявлениями о преступлениях в органах внутренних дел в недостаточной степени регламентирована и технически обеспечена.

В целях усовершенствования данного направления деятельности предлагается рассмотреть вопрос о разработке специального программного обеспечения и алгоритма ускоренного прохождения заявления от заявителя до уполномоченного должностного лица, а также внести изменения или переработать действующие нормативные правовые акты МВД России с учетом нового алгоритма.

Реализация предложенных мер позволит значительным образом повысить оперативность реагирования на сообщения граждан о преступлениях и снизить количество повторных обращений граждан, а также снимет с подразделений делопроизводства и режима несвойственную функцию по приему заявлений о преступлениях.

Копцов Сергей Васильевич,
кандидат социологических наук,
старший преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

ОСОБЕННОСТИ РАССМОТРЕНИЯ ОТДЕЛЬНЫХ КАТЕГОРИЙ ОБРАЩЕНИЙ ГРАЖДАН

Среди приоритетных задач, которые стоят перед ОВД, представляется соблюдение сотрудниками полиции служебной дисциплины и законности, и ключевым значением является соблюдение законных прав и интересов граждан.

Именно поэтому, как никогда, в числе многих других одной из задач МВД России является решение проблемы сокращения количества обращений на действия сотрудников полиции, поскольку очевидно, что качественное рассмотрение обращений граждан также способствует укреплению доверия между ОВД и населением, а граждане, имея возможность обратиться с проблемой или вопросом, ощутят поддержку и понимание со стороны ОВД. Это помогает укрепить сотрудничество и совместную работу в решении проблем и обеспечении безопасности общества.

Кроме того, рассмотрение обращений граждан также является важным инструментом для предотвращения и выявления коррупции, недостатков и нарушений в работе ОВД, а сами граждане могут сообщать о случаях неэффективности, произволе и нарушениях со стороны сотрудников ОВД, что будет способствовать поддержанию честности и ответственности в их работе.

Так, в 3-ем квартале 2024 года в адрес МВД России, а также его руководства поступило около 84 082 обращений от граждан и организаций, что на 0,01 % больше сравнительно с идентичным промежутком времени прошлого года, где результат был 84 072.

Количество обращений, которые были перенаправлены из Управления Президента РФ по работе с обращениями граждан и организаций увеличилось на 6,8 % (с 21 857 до 23 333), а вот из Правительства Российской Федерации на 7 % (с 2 212 до 2 367).

Значительное изменение наблюдалось в объеме обращений с официального сайта МВД России, так их величина возросла на 96 % (с 39 833 до 78 055).

Наибольшая активность граждан зафиксирована в следующих субъектах Российской Федерации: г. Москве (19 002), Московской области

(10 891), г. Санкт-Петербурге (5 906), Краснодарском крае (5 518), Свердловской области (2 922), Республике Татарстан (2 533), Ростовской области (2 477), Республике Башкортостан (2 040)[1].

К сожалению, как мы видим, количество самих фактов нарушений требований нормативно-правовых актов при рассмотрении обращений граждан увеличивается количества, что несомненно ведет к увеличению количества обращений на действия сотрудников полиции, другими словами отдельных видов обращений.

Напомню, что к отдельным обращениям, согласно Приказу МВД России от 12.09.2013 №707[2] относятся 12 основных видов[3]:

1. Обращения о неправомерном поведении, которые были совершенны сотрудниками ОВД.

2. Сведения, содержащие информацию о коррупционных действиях должностных лиц ОВД, либо об их личной заинтересованности, которая в дальнейшем может привести к конфликту интересов.

3. Из органов государственной власти, органов местного самоуправления и судов, которые связанны с рассмотрением исков в судах общей юрисдикции.

4. Касающиеся процессуальных вопросов по делам об административных правонарушениях, которые находятся в производстве должностных лиц Органов Внутренних Дел.

5. Касающиеся обжалования действий должностных лиц ОВД по применению законодательства об административных правонарушениях, которые не являются предметом самостоятельного обжалования, являясь тесно связанными с делом об административном правонарушении (жалоба на применение указанных в главе 27 КоАП РФ мер обеспечения производства по делу; жалоба на протокол по делу, по которому было вынесено постановление).

6. Жалобы, поступившие в порядке статьи 124 УПК РФ, ходатайства по уголовным делам, находящимся в производстве органов предварительного следствия и дознания системы МВД России (об ознакомлении с заключением эксперта; о приобщении доказательств; о дополнительном допросе лиц).

7. Проблема с нарушением установленного порядка оказания государственных услуг.

8. Обращение сотрудника по форме рапорта или докладной записки с заявлением, предложением, а также жалобой (в том числе об отказе в предоставлении отпуска, обжаловании дисциплинарного взыскания, уведомлениями о фактах склонения к совершению коррупционных правонарушений).

---

[1] Данные Информационного центра МВД России

[2] Далее Инструкция

[3] Глава VIII приказа МВД России от 12.09.2013 №707

9. Сообщения, содержащие аудио- или видеозаписи, а также URL-адреса, ведущие к хранилищам аудио-, видео- или иных информационных файлов.

10. Газеты, журналы и другие печатные издания, поступившие от гражданина без приложения обращения с изложением существа просьбы.

11. Анонимные обращения, содержащие сведения о подготавливаемом, совершаемом или совершенном противоправном деянии, а также о лице, его подготавливающем, совершающем или совершившем.

12. Анонимные заявления, содержащие информацию о совершенном или готовящемся террористическом акте.

Регистрация подобных обращений производится в порядке, определенном Инструкцией, а их рассмотрение осуществляется в соответствии с нормативными правовыми актами МВД России.

Ниже представлен детальный разбор процесса их регистрации.

Согласно Инструкции, осуществляется регистрация, учет и принятие организационных решений по обращениям, касающимся нарушений порядка предоставления государственных услуг, поступившим в рамках пункта 27 Инструкции, если их рассмотрение не предусмотрено Федеральным законом.

Данные обращения рассматриваются по существу в порядке, установленном законодательными актами Российской Федерации. В учетной форме в сокращенном виде указывается вид и номер нормативного акта, регулирующего порядок их рассмотрения.

Заявление, предложение, жалобы и иные обращения, поступившие от сотрудников по форме рапорта или докладной записки, регистрируются и учитываются в порядке, установленном Инструкцией. Их рассмотрение осуществляется согласно законодательству РФ и НПА МВД России, за исключением случаев с особым порядком. В учетной форме указывается "рапорт".

Обращения, с аудио- и (или) видеозаписями, ссылками (гиперссылками) на контент интернет-сайтов, являющихся хранилищем файлов аудио- и (или) видеозаписей и иных информационных файлов проходят регистрацию и учет в соответствии с Инструкцией. Однако, рассмотрение таких обращений по существу производят при наличии текстового изложения его сути. В противном случае гражданину необходимо направить уведомление о невозможности рассмотрения отправленного им обращения, как некорректно изложенного, согласно 76 пункту Инструкции.

Газеты, журналы и иные печатные материалы, которые поступили от гражданина без сопроводительного обращения с изложением сути просьбы, не подлежат регистрации, а также рассмотрению в порядке, установленном Инструкцией.

Анонимные обращения, которые содержат информацию о подготавливаемом, совершаемом и (или) уже совершенном противоправном деянии,

а также о лице, его подготавливающем, совершающем или совершившем, проходят регистрацию в порядке, установленном Инструкцией, и направляются в соответствующие подразделения МВД России или другие государственные органы в соответствии с компетенцией. При этом в учетной форме в графе об исполнении делается отметка «анонимное».

Анонимные заявления о совершенном или готовящемся террористическом акте, в кратчайший срок докладываются уполномоченным сотрудником подразделения делопроизводства руководителю территориального органа, далее в соответствии с его резолюцией передаются в дежурную часть, где регистрируются в книге учёта сообщений о преступлениях, административных правонарушениях и происшествиях (КУСП).

В центральном аппарате МВД России оригинал анонимного заявления, содержащего информацию, указанную в пункте 130 Инструкции, направляется в территориальный орган (межрегионального или регионального) уровня, а копии этого обращения передаются в аппарат заместителя Министра внутренних дел РФ, который ответственный за данное направление деятельности, а также в ФСБ РФ.

Руководитель ОМВД принимает решение об обоснованности проведения проверки по факту поступления анонимного сообщения, если оно не содержит сведений, которые изложены в 130 пункте Инструкции.

Стоит отметить, если в ходе осуществления проверки по жалобе определено, что в качестве гражданина указано лицо, которое не обращалось в ОВД, либо в его обращении были названы вымышленные адрес и (или) фамилия, имя, отчество, то жалоба признается анонимной[1].

Если из другого органа внутренних дел поступило идентичное обращение, являющееся копией или же дубликатом раннее рассмотренного, срок рассмотрения которого истек, то оно рассматриваться не должно. В этом случае гражданину необходимо направить уведомление о ранее направленном ответе.

Переписка с гражданином по раннее рассмотренному вопросу, можно прекратить по решению руководителя ОВД на основании мотивированного заключения (в центральном аппарате МВД - докладной записке) о признании необоснованности обращения. Далее гражданину необходимо направить письменное уведомление о прекращении с ним переписки с подробным и обоснованным решением, принятых по поставленным вопросам, и указанием реквизитов предыдущих ответов[2].

Последующие обращения проверяются на предмет отсутствия новых доводов и обстоятельств, требующих дополнительной проверки, и без рассмотрения по существу списываются в дело по докладной записке сотруд-

---

[1] П.133 Инструкции

[2] П.135 Инструкции

ника подразделения, осуществлявшего рассмотрение предыдущих обращений, или сотрудника подразделения делопроизводства. Ответы на такие обращения не даются[1].

Заявление о прекращении рассмотрения обращения должно быть зарегистрировано в установленном порядке. Оно считается поддержанным, когда сведения о наличии нарушений закона, требующих принятия мер реагирования не установлены. В случае выявления признаков неправомерных действий или бездействия сотрудников, назначается служебная проверка. Заявление о прекращении рассмотрения обращения приобщается к материалу первого обращения, о чем необходимо уведомить гражданина.

Обобщенные результаты рассмотрения типовых обращений размещаются на официальных ресурсах ОВД и в средствах массовой информации, но ответы на конкретные типовые обращения направляются каждому гражданину персонально в соответствии с процедурой.

Как правило, основными нормативными документами являются: Федеральный закон Российской Федерации от 30.11.2011 №342 «О службе в органах внутренних дел российской федерации и внесении изменений в отдельные законодательные акты российской федерации», Указ Президента РФ от 14 октября 2012 г. № 1377 «О Дисциплинарном уставе органов внутренних дел Российской Федерации», а также Приказ МВД России от 26 марта 2013 г. N 161 «Об утверждении Порядка проведения служебной проверки в органах, организациях и подразделениях Министерства внутренних дел Российской Федерации».

Среди наиболее распространенных нарушений принципов полноты, всесторонности и объективности при рассмотрении обращений выделяют:

– замещение содержания проверки по обращению заключением служебной проверки;

– описательная часть заключений не содержит объективного анализа установленных фактов и обстоятельств, либо сведений и материалов, подтверждающих или опровергающих доводы заявителей;

– направление ответов ненадлежащего качества (ответ дан не по существу всех поставленных вопросов в обращении; изобилие нерасшифрованных аббревиатур;

– наличие ошибок в тексте или данных заявителя;

– отсутствие ссылок на НПА, послужившие основанием для принятия решения и т.д.).

Среди главных нарушений, допускаемых при принятии организационного решения в процессе рассмотрения обращений, выделяют:

Направление обращения к лицу или органу, чьи действия/бездействие обжалуются, является обычным делом. Но, затруднения при определении ответственного исполнителя могут привести к неверному перенаправлению

---

[1] П.136 Инструкции

между подразделениями. Это влечет за собой сокращение времени на рассмотрение и формальный подход к делу со стороны исполнителя, чтобы уложиться в сроки.

Много затруднений возникает у сотрудников ОВД при принятии решения о прекращении переписки, в частности:

– факторы, обуславливающие прекращение;

– корректность оформления;

– кто является уполномоченным лицом для подписания заключения;

– как корректно составить ответ заявителю и каким образом рассматривать последующие обращения от заявителей, с которыми переписка была завершена.

Мы уже не раз разговорили об указанных причинах, которые из года в год повторяются, а их количество увеличивается.

Рассмотрим основные направления решения проблемных вопросов:

– на информационных стендах, размещенных в общедоступных для граждан местах, необходимо размещать информацию, содержащую сведения о порядке и сроках рассмотрения обращений, а также о процедуре обжалования действий (бездействия) и решений сотрудников ОВД, с целью повышения правовой грамотности граждан.

– применение возможностей официального сайта ГУ МВД России по Краснодарскому краю для освещения результатов оперативно-розыскных и профилактических мероприятий, проведения разъяснительной работы среди населения в отношении законодательных и иных нормативных правовых актов, относящихся к ведению МВД России.

– в рамках акции «Правовое информирование граждан» активно проводить мероприятия «Прямая линия с населением», в результате которого в телефонном режиме осуществлялось консультирование граждан по вопросам, входящим в компетенцию органов внутренних дел, а также личный прием граждан руководством всех должностных категорий.

Ларина Алевтина Юрьевна,
преподаватель кафедры информационной
безопасности Краснодарского
университета МВД России

АНАЛИЗ КОНТРОЛЯ ЗА ИСПОЛНЕНИЕМ ПОРУЧЕНИЙ РУКОВОДИТЕЛЯ

Контроль за исполнением поручений руководителя является одним из основных методов повышения эффективности управленческой деятельности, обеспечивает качественную исполнительскую дисциплину и служит базой для повышения результатов работы.

В соответствии с Инструкцией по делопроизводству в органах внутренних дел Российской Федерации, утвержденной приказом МВД России от 02.09.2024 № 515[1], *контроль исполнения документов* (поручений) представляет собой совокупность действий, реализуемых в целях их своевременного и качественного исполнения.

Контроль за исполнением поручений как процесс включает в себя:

– постановку документов на контроль;

– осуществление промежуточного, заключительного контроля;

– снятие с контроля;

– сбор, учет, обобщение и анализ сведений о выполнении;

– информирование руководителей об исполнении.

Выделяют следующие виды контроля за исполнением поручений:

Промежуточный – отслеживание последовательности действий по выполнению поручений.

Заключительный – итоговая проверка выполнения сотрудником поручения руководителя.

В приказе МВД России представлен перечень должностных лиц, на которых возлагается ответственность за осуществление контроля:

– руководители всех уровней, к компетенции которых относится непосредственное исполнение поручения;

– субъекты контроля, по части соблюдения сотрудниками сроков исполнения поручений.

В системе МВД России субъектами контроля признаются: Департамент делопроизводства и работы с обращениями граждан и организаций, организационно-аналитический департамент и договорно-правовой департамент МВД России. В подразделениях органов внутренних дел данным вопросом занимаются отделы делопроизводства и режима, а также подразделения, которые выполняют работу по анализу, планированию и контролю.

---

[1] Далее – приказ МВД России

Стоит отметить, что срок исполнения поручения исчисляется в календарных днях с момента поступления документа:

– в сроки и в порядке, установленные законодательными или иными нормативно-правовыми актами;

– в течение 1-2 дней, если в тексте документа имеется пометка «весьма срочно» или «незамедлительно»;

– в 3-х дневный срок, в случае наличия пометки «срочно»;

– в 10-ти дневный срок, если есть пометка «оперативно»;

– в указанный в тексте документа срок (при наличии);

– не более 1 месяца, если не установлена конкретная дата исполнения поручения.

К особенностям осуществления контроля за исполнением поручений относится возможность продления срока исполнения документа, если исполнитель не успевает выполнить поручение в установленный срок, но решение о его продлении может принять руководитель, который дал данное поручение, или уполномоченное на принятие такого решения лицо.

Тем не менее, не смотря на простую структуру организации исполнения поручений в учреждениях и подразделениях полиции существует совокупность проблем, влекущих к неисполнению в срок поручений руководителей.

Анализ контроля за исполнением поручений руководителя показал, что среди причин нарушения сроков исполнения документов выделяют:

– Человеческий фактор (по состоянию здоровья; недостаточная осведомлённость в нормативных правовых актах, регламентирующих делопроизводство и иные сферы деятельности; личная недисциплинированность сотрудника);

– «Затянувшийся» маршрут согласования и подписания документа (в качестве примера: внеплановая командировка должностного лица).

– низкий уровень укомплектованности штата некоторых служб, и как следствие, высокая загруженность сотрудников.

Вышеперечисленные причины нарушения сроков исполнения поручений руководителя могут привести в том числе и к нарушению прав и свобод граждан. А это в свою очередь может привести не только к судебным разбирательствам, но и породить в обществе недоверие к органам внутренних дел со стороны граждан.

В заключении отмечу, что обеспечению системного и качественного контроля за исполнением поручений способствует:

– четкое разделение труда в аппарате;

– грамотно составленное положение о подразделении делопроизводств, должностные инструкции сотрудников, обеспечивающие обозначение ответственного исполнителя;

– конкретные и однозначные формулировки решений, фиксируемых в резолюциях;

– высокое качество подготовки документов.

Разиньков Александр Сергеевич,
начальник отдела по борьбе с организованной
преступностью, заместитель начальника УУР ГУ
МВД России по Краснодарскому краю;
Куликов Кирилл Сергеевич
старший оперуполномоченный ЦПЭ
ГУ МВД России по Краснодарскому краю

МЕТОДЫ ПРЕДУПРЕЖДЕНИЯ РАСПРОСТРАНЕНИЯ ИДЕОЛОГИИ «СКУЛШУТИНГА» С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

В современной России наблюдается возрастающая бурная активность экстремистских настроений среди пользователей информационно-телекоммуникационных систем, в том числе в сети Интернет. В средствах массовой информации и ресурсах сети Интернет все чаще появляются новости о политическом экстремизме, о террористических актах и запрещенных на территории Российской Федерации террористических организациях, а в свете последних событий признание некоторых СМИ - иностранными агентами, ставит под вопрос об истинности и правдивости распространяемых сведений. Стоит отметить, что экстремистская идеология быстрее всего распространяется среди молодежи, связано это с тем, что в основном именно люди молодого возраста больше подвержены психологическому воздействию со стороны негативного контента, в связи свойственной данной группе психологии максимализма и подражания.

В последнее время на территории Российской Федерации все чаще встречаются факты насилия, совершаемые в образовательных учреждениях. При этом, стоит понимать, что во многих случаях данные факты, сопряженные с массовыми убийствами и культами фанатичности к определенным субкультурам, в том числе запрещенными. При этом в социальных сетях и отдельных форумах сети Интернет молодежью данные факты рассматриваются ни как что-то плохое, а как норма ответных действий со стороны лиц, подвергающихся буллингу, а лица совершающие данные действия представляют в свете «героев».

Многие авторы в своих работах разделяют понятие «скулшутинга» и «колумбайна», связывая это с тем, что «скулшутинг» это явление, связанное с непосредственным производством противоправной деятельности и она может быть направленно в отношении конкретного лица в образовательной системе, а «колумбайн» носит неформальный характер среди молодежных групп, формируя идею беспорядочных убийств в образовательных организациях.

Само слово «скулшутинг» имеет американское происхождение от слова «school shooting» и переводится дословно как школьная стрельба.

Происхождение данного слова не просто так берет свое начало из США, связанно это с тем, что именно в этой стране зародилось субкультура «колумбайна» и предалась огласка, которая позволила сформировать в молодежной среде движение.

В 1999 году в штате Колорадо, двое учеников Эрик Харрис и Дилан Клиболд, пришли в школу Колумбайн в которой обучались и убили 13 человек и ранили еще 24 человека. Именно данный факт положил основу для субкультурного движения «колумбайн», но возникает справедливый вопрос, неужели ранее не совершались факты массовых убийств в образовательных организациях во всем мире? Конечно такие факты имели место быть, к примеру, в 1989 году Патрик Эдуард Петри, вооружённый автоматом АК, пришел в Кливленда в США и устроил стрельбу в результате которой погибло пятеро детей и более двадцать человек были ранены, но именно массовое убийство произошедшее в школе Колумбайн создало большой общественный резонанс и связанно это с такими факторами как: Спланированность действий, медийность, стилистика, наличие обиды.

Безусловно, данные факты сформировали определённую субкультурность, которая в последующем легла в идеологию данного экстремистского феномена. Культ тех действий, совершенных Эриком Харрисом и Диланом Клиболдом переросли из фанатичности в подвижную пропаганду совершения актов массовых убийств в образовательных учреждениях. Связанно это в первую очередь с тем, что стрельба в школе Колумбайн это не просто поведение двух молодых людей, потерявших рассудок, это в первую очередь выстроенная идеология.

Наиболее резонансным и с явными признаками фанатичности к «скулшутингу» стал случай, произошедший в Керченском политехническом колледже, где студент Владислав Росляков, подражая идеологии «колумбайна», совершил массово убийство учащихся и персонала колледжа, в количестве двадцати одного человека, пострадавшими стали шестьдесят семь человек. При этом Владислав имел все атрибуты «скулшутера», описанные нами ранее, а именно: заранее подготовленный план действий; публичное распространение информации о подготавливаемом акте; одежду схожую с Эриком Харрисом, оружие по типу использованное им же; проблемы в учебном заведении; окончание актом деяния суицидом (при этом местом совершения суицида Владислав Росляков выбрал такое же, как и его кумиры в библиотеке колледжа).

Безусловно, приведённый пример на территории Российской Федерации, позволяет сделать вывод, что молодой человек перед совершением противоправного деяния целенаправленно изучали контент, по средством сети Интернет, который можно отнести к «скулшутингу».

Становится очевидным, что сеть Интернет влияет на многие социальные процессы общества, в том числе на способы распространения экстре-

мистки материалов. В частности, лица, действующие против интересов Российской Федерации, вливают в огромном объеме по средством социальных сетей и мессенджеров пропаганду идей «скулшутинга», раскручивая идеи по средством прямого общения в личных сообщениях или специальных площадках в сети Интернет с молодыми людьми, подверженными данными идеями.

В настоящее время молодое поколение все чаше использует для коммуникации и общения социальные сети и мессенджеры, зачастую скрывая свои данные под ник-именами, что ставит определенные трудности перед сотрудниками правоохранительных органов. В связи с чем грамотное выявление приверженности в сети Интернет позволяет своевременно реагировать и предупреждать проявления насилия.

Приведенный контент-анализ Интернет ресурсов, социальных сетей и мессенджеров, пропагандирующих идеологию массовых убийств в образовательных организациях, позволил выделить следующие характерные особенности ведения страниц пользователей приверженных к идеологии «скулшутинга» и «колумбайна».

1. Упоминание на страницах в социальных сетях и мессенджерах имен «кумиров» (Дилана Клиболда, Эрика Харриса, Владимира Рослякова и др.), совершивших массовые убийства, их изображение, выставление их как героев, желание повторить их судьбу, зачастую подражание в внешнем виде.

2. Упоминание цифр и дат, имеющих значение для представителей «колумбайна», к примеру: 20.04.1999 – стрельба в школе «Колумбайн»; 17.10.2018 – стрельба, в Керчи Владиславом Росляковым; 11.05.2021 – стрельба в Казанской гимназии Ильназом Галявиевым; 20.09.2021 – стрельба в Пермском Государственном Национальном исследовательском институте, Тимуром Бекмансуровым.

3. Наличие на странице публикаций с изображением моментов совершения «скулшутинга» Эриком Харрисом и Диланом Клиболдом.

4. Записи блогов «кумиров», к примеру: фраза «Ich bin Gott» переводимая как «Я Бог» употребляемая в видео дневнике Эриком Харрисом.

5. Высмеивание системы образования, унижение преподавателей, которое совершается публично на странице социальной сети в целях предания огласки.

6. Размещение атрибутики и вещей присущих «кумирам», к примеру футболки, с надписью «Ненависть», «Естественный отбор», которые носили Эрик Харрис и Дилан Клиболд.

7. Размещение на странице видеозаписей с фрагментами нападений на школу, в том числе монтирование видеоклипов с наложением музыки, к примеру, Oxxxymiron – «Последний звонок»; музыка групп- Skabbibal, KMFDM, в жанре блек метал.

8. Публикации стрельбы из оружия, тактические характеристики, в частности из оружия помповое ружьё Savage-Springfield 67H, самозарядного карабин Hi-Point 995, обреза двуствольного ружья Stevens 311D, 9-миллиметрового самозарядного пистолета TEC-9.

9. Фрагменты из художественных и документальных фильмов, снятых по мотивам событий в школе «Колумбайн»: «Слон», «Класс», «Боулинг для Колумбины».

При этом также следует уделять внимание внешнему виду, который может совпадать с внешним видом вышеупомянутых «кумиров», а именно образа одежды, который включает в себя: берцы; короткие джинсы; плащ; футболки с вышеупомянутыми нанесёнными фразами; круглые солнцезащитные очки.

Профилактика идеологии насилия и массовых убийств в образовательных организациях проводится не только в формате реагирования на произошедшие факты, но и в формате первичной профилактики включающая в себя своевременное предупреждение фатов агрессии, формирование у подрастающего поколения правильных ценностных ориентиров, помощь лиц, оказавшихся в трудной жизненной ситуации.

В связи с чем можно выстроить следующие пути профилактики и предупреждения идеологии насилия и массовых убийств в образовательных организациях:

1. Проведение классных часов по типу тренингов, на которых существует возможность научить подростков и обучающихся способом взаимодействия друг с другом без применения насилия, минимизация агрессии, стремление участия всех учащихся.

2. Благоприятный климат в семье. Понимающая семейная обстановка крайне важна для непростого переходного периода подросткового возраста, поэтому членам семьи предлагается осветить основные якорные моменты в развитии данного возрастного этапа, которые требуют более трепетного отношения, к примеру, на родительских часах или собрания.

3. Ориентированность образовательного учреждения не только на повышение качества учебного процесса, но и на создание психологического комфорта для обучающихся, их социализацию и формирование неприятия насилия в любых его формах.

4. Выявление и пресечение распространения противоправного контента. Безусловно данный способ связан с тем, что, искоренив корень проблемы, непосредственны источник распространения деструктивной модели поведения как колумбайн мы сможем качественно воздействовать на возможные факты распространения данного явления, при этом следует понимать, что данный способ противодействия основываются на мониторинге сети Интернет.

Деструктивные группы, пропагандирующее субкультуру колумбайн, запрещены на территории Российской Федерации как побуждающие детей

к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству либо жизни и (или) здоровью иных лиц.

В целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». Созданием, формированием и ведением реестра занимается федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Роскомнадзор). Основанием для включения в реестр и, соответственно, блокировки такого сайта является решение суда либо уполномоченных федеральных органов исполнительной власти.

В связи с проведённым контент-анализом Интернет ресурсов, социальных сетей и мессенджеров, пропагандирующих идеологию массовых убийств в образовательных организациях, позволил выделить следующие характерные особенности ведения страниц пользователей приверженных к идеологии «скулшутинга» и «колумбайна», можно своевременно блокировать контент, который может попасть на обозрение молодых людей, тем самым предупреждать распространение идеологии.

Власенко Александра Владимировна,
доцент кафедры информационной безопасности
Краснодарского университета МВД России

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЛОПРОИЗВОДСТВЕ ОВД: ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ПРОЗРАЧНОСТИ И БЕЗОПАСНОСТИ

С развитием цифровых технологий перед органами внутренних дел (ОВД) встают новые задачи в области управления документацией и информационной безопасности.

По мере увеличения объемов данных и повышения требований к безопасности особое значение приобретает использование инновационных технологий.

Одной из таких технологий является блокчейн, который может значительно повысить уровень прозрачности и безопасности в делопроизводстве ОВД.

В этой статье описываются основные принципы, преимущества и успешные применения технологии блокчейн, а также проблемы, с которыми сталкиваются ОВД при внедрении технологии блокчейн.

Блокчейн - это децентрализованная база данных, которая хранит информацию в виде цепочки блоков, связанных между собой криптографическими методами.

Каждый блок содержит информацию о транзакциях и краткое содержание предыдущего блока, и изменить эти данные без согласия всех участников сети невозможно.

Структура блокчейна состоит из серии блоков, каждый из которых содержит временную метку, хэш предыдущего блока, заголовок блока, содержащий уникальный идентификатор, основное содержимое блока, хранящее транзакции и данные, и криптографическую подпись, гарантирующую целостность данных.

Принципами блокчейна являются децентрализация, неизменяемость и прозрачность.

Поэтому в блокчейн нет централизованного органа, что снижает риск манипуляций и злоупотреблений.

Когда блок добавляется в блокчейн, гарантируется высокая степень информационной безопасности, поскольку данные не могут быть изменены или удалены.

Доверие между сторонами поощряется, поскольку все участники сети могут видеть все транзакции.

Рассмотрим преимущества технологии блокчейн в управлении делами ОВД.

Одно из главных преимуществ технологии блокчейн - высокая степень информационной безопасности.

Данные, записанные в блокчейн, невозможно изменить или удалить, что снижает риск утечки и подделки документов.

Это особенно важно для органов внутренних дел, деятельность которых связана с обработкой конфиденциальной информации.

Данные защищены от несанкционированного доступа, так как зашифрованы с помощью новейших методов шифрования.

Все изменения и транзакции отслеживаются в режиме реального времени, что позволяет контролировать и отслеживать действия сотрудников.

Блокчейн обеспечивает полную прозрачность всех операций и позволяет отслеживать все изменения в данных.

Это помогает управлять процессом управления делами, а также привлекать сотрудников ОВД к ответственности. Наличие полной истории изменений предотвращает споры и недопонимание между различными сторонами.

Прозрачность транзакций помогает улучшить коммуникацию между различными подразделениями ОВД и другими государственными органами.

Использование технологии блокчейн позволяет сократить расходы на управление документами.

Автоматизация процессов, связанных с обработкой и хранением документов, позволяет сократить время и ресурсы, затрачиваемые на выполнение рутинных задач.

Автоматизация рутинных задач, таких как контроль и обработка документов, позволяет высвободить время сотрудников для выполнения более важных задач.

На сегодняшний день примеры успешного внедрения блокчейна наблюдаются в разных странах.

Например, Эстония является одним из лидеров в области оцифровки государственных услуг. В стране внедрена система электронного правительства на основе блокчейна, которая обеспечивает безопасное хранение и обработку данных граждан.

Граждане используют электронные сертификаты, которые хранятся в блокчейне и гарантируют их безопасность и подлинность.

Блокчейн используется для предоставления различных государственных услуг, таких как регистрация бизнеса, налоговые декларации и голосование.

Россия также экспериментирует с использованием блокчейна для обеспечения прозрачности и безопасности правительства.

Проект «Госуслуги» изучает возможности использования технологии блокчейн для повышения безопасности и прозрачности государственных услуг.

В России существует несколько пилотных проектов, направленных на внедрение технологии блокчейн в различных отраслях, в том числе в органах внутренних дел.

Некоторые из них описаны ниже:

1. В Москве реализуется проект «Госуслуги на блокчейне».

Данный проект изучает возможность использования блокчейна для повышения прозрачности и безопасности государственных услуг.

Цель проекта - разработать прототип системы, которая позволит гражданам безопасно взаимодействовать с государственными органами и получать услуги через блокчейн.

2. В Татарстане реализуется проект по внедрению электронного паспорта для граждан на основе технологии блокчейн.

Проект направлен на создание надежной и безопасной системы идентификации граждан, которая позволит улучшить доступ к государственным услугам и повысить уровень безопасности данных.

3. В Санкт-Петербурге реализуется проект по использованию технологии блокчейн в рамках инициативы «Цифровая экономика».

В рамках проекта будет изучено применение блокчейн-технологий для управления данными в различных областях, включая здравоохранение и образование.

4. Свердловская область инициировала проект по внедрению технологии блокчейн в документооборот государственных учреждений.

Целью проекта является автоматизация процессов, связанных с обработкой и хранением документов, а также повышением безопасности обрабатываемых данных.

5. В Калужской области реализуется проект, направленный на использование смарт-контрактов для автоматизации административных процессов.

В рамках проекта разрабатываются прототипы смарт-контрактов для различных государственных услуг.

Данные проекты являются примерами применения технологии блокчейн в России и могут послужить основой для дальнейших исследований и внедрения этих технологий в органах внутренних дел и других сферах государственного управления.

Пилотные проекты по внедрению технологии блокчейн в органах внутренних дел реализуется и в Краснодарском крае.

К числу таких проектов относится проект «Безопасный город».

Еще в 2014 году Правительство Российской Федерации утвердило концепцию аппаратно-программного комплекса «Безопасный город» — это совокупность технических и программных средств, которые способны облегчить работу ведомств и служб по предотвращению и устранению явлений, угрожающих жизни и здоровью граждан. За десять лет с момента раз-

вития системы «Безопасный город» количество зарегистрированных преступлений сократилось вдвое. В десять раз, сократилось число зарегистрированных угонов, а раскрываемость преступлений выросла в два раза.

Рассмотрим территорию муниципального образования г. Краснодара, здесь с 2014 года реализована программа по построению и функционированию системы «Безопасный город». В состав комплекса входит свыше 1100 камер видеофиксации, а с весны 2021 года функционирует интеллектуальная система видеонаблюдения, которая реализована на скоростных шоссе, позволяя быстрее и эффективнее обрабатывать видеопоток и автоматически фиксирует совершенное правонарушение.

Система «Безопасный город» многофункциональна, даже в борьбе с противоправными явлениями. Статистика говорит о том, что в 2022 году при помощи обработанных системой данных сотрудникам удалось раскрыть свыше 360 преступных деяний и более 980 административных правонарушений.

В рамках этого проекта технология блокчейн интегрируется для повышения безопасности и эффективности работы правоохранительных органов.

Проект предусматривает использование современных технологий для мониторинга и анализа данных, что помогает улучшить реагирование на происшествия и повысить уровень безопасности в обществе.

Также в Краснодарском крае реализуется проект по внедрению электронного документооборота, направленный на автоматизацию процесса документооборота в ОВД с использованием технологии блокчейн. Это позволит повысить прозрачность и безопасность документооборота, а также сократить время обработки документов.

В рамках проекта «Умные контракты» для ОВД рассматривается возможность использования смарт-контрактов для автоматизации различных процессов в органах внутренних дел, таких как регистрация граждан, обработка заявлений и взаимодействие с другими государственными структурами.

Смарт-контракт – это компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн.

Технология смарт-контрактов предлагает программный способ описания взаимоотношений и автоматических действий между сторонами. Одной из особенностей смарт-контракта является его децентрализованная природа и однозначная автоматическая исполняемость — единожды размещенный на децентрализованной платформе, такой контракт будет существовать и исполняться всегда (при наступлении соответствующих событий), пока будет существовать такая платформа.

Единожды размещенный в блокчейн сети, смарт-контракт будет всегда выполняться единообразно и автоматически, при наступлении запрограммированных событий.

Безопасность и единообразность исполнения смарт-контрактов обеспечивается децентрализованной природой и алгоритмами консенсуса блокчейн

сети. Ни одна из сторон смарт-контракта не имеет возможности внести изменения в смарт-контракт, после момента размещения его в блокчейн сети.

Смарт-контракты позволяют исключить неэффективных, не несущих полезной нагрузки посредников из цепочек поставок. Транзакции проходят автоматически без дополнительного одобрения сторонами смарт-контракта.

Все перечисленные пилотные проекты направлены на улучшение работы органов внутренних дел, повышения уровня безопасности и прозрачности, а также оптимизацию процесса взаимодействия с гражданами.

Рассмотрим основные преимущества внедрения технологии блокчейн в ОВД, в частности в рамках таких пилотных проектов, как «Безопасный город», «Электронный документооборот» и «Умные контракты».

Блокчейн прежде всего обеспечивает высокую степень защиты информации благодаря централизованному характеру хранения данных и криптографическим методам.

Все транзакции записываются в блокчейн и могут быть проверены, что повышает доверие общества и сокращает возможности для коррупции.

Использование смарт-контрактов автоматизирует многие административные процессы, сокращая время на обработку заявлений и документов.

Смарт-контракт – это компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн. Технология смарт-контрактов предлагает программный способ описания взаимоотношений и автоматических действий между сторонами.

Технология блокчейн упрощает доступ граждан к услугам ОВД, позволяя им быстро и безопасно подавать заявления и получать информацию.

Автоматизация и оптимизация процессов позволяют сократить расходы на обработку данных и документооборот.

Использование блокчейн-технологий для сбора и анализа больших объемов данных позволяет выявлять тенденции преступности и разрабатывать более эффективные меры по ее предотвращению.

Наряду с преимуществами существуют и недостатки:

Внедрение технологии блокчейн требует значительных затрат на обучение персонала, модернизацию инфраструктуры и разработку программного обеспечения.

Технология блокчейн может столкнуться с проблемами в сфере регулирования, поскольку законодательство не всегда успевает за технологическими инновациями.

Некоторые блокчейн-системы имеют проблемы с масштабируемостью, что может ограничить их использование в крупных проектах.

Внедрение новых технологий может привести к зависимости от технологий, что может нарушить работу ОВД в случае сбоя системы.

Кибербезопасность встроена в технологию блокчейна из-за ее изначальной природы как децентрализованной системы, построенной на принципах безопасности, конфиденциальности и доверия.

Децентрализованные системы хранения файлов на основе блокчейна распределяют данные по сети, снижая риск возникновения единой точки отказа.

Это не только повышает безопасность конфиденциальных файлов, но и обеспечивает конфиденциальность, сводя к минимуму подверженность данных потенциальным нарушениям.

Для использования технологии блокчейн требуются специалисты.

Это эксперты по технологии блокчейн, которые разрабатывают, внедряют и управляют системами и приложениями блокчейн.

Это включает в себя разработку блокчейн, создание смарт-контрактов, разработку децентрализованных приложений, поддержку инфраструктуры блокчейн, интеграцию систем блокчейн в ОВД, интеграцию систем блокчейн в различные отрасли, а также в том числе консультирование по вопросам внедрения и оптимизации блокчейн-решений.

Профессия требует глубоких знаний в области информационных технологий, криптографии, безопасности данных и программирования.

Однако для успешного внедрения необходимо преодолеть существующие проблемы, включая юридические и организационные аспекты.

Важно продолжать изучать потенциал технологии блокчейн и адаптировать ее к конкретным потребностям ОВД.

Успех этих усилий будет зависеть от правильного подхода к внедрению, учета возможных рисков и активного сотрудничества с гражданами и другими государственными органами.

Куминов Михаил Владимирович,
старший преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ С ИСПОЛЬЗОВАНИЕМ СЕРВИСА ЭЛЕКТРОННОЙ ПОЧТЫ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Первые упоминания об электронном документообороте были в 1970-х годах – это были первые компьютерные системы управления документами, где основная функция — это автоматизация бумажного потока. В 1980-е годы возникли возможности использовать более сложные и гибкие системы для обработки текстов, это аналог современных текстовых редакторов (программные продукты, позволяющие создавать и редактировать электронные текстовые документы). В 1990-е годы, с развитием «Интернета» и появление электронной почты начался создаваться электронный обмен данными (EDI), который стал предшественником электронного документооборота. И уже в 2000-е годы разработаны и стали широко доступными первые системы электронного документооборота. Данные системы стали использовались для создания, хранения, изменения и управления электронными документами. Взамен локальных хранилищ пришли облачные технологии. Начиная с 2010-х годов развитие мобильных технологий и увеличение объема данных, повлекло увеличение масштаба использования электронного документооборота. Появляется необходимость в создании способности интеграции систем, тем самым придавая им новых свойств как надежность и безопасность. А с 2020-го года, в разгар пандемии COVID-19 появилась острая необходимость бесконтактной передачи документов с возможность их подписания обеими сторонами.

Для начала надо вспомнить что такое «электронный документооборот» (ЭДО) и «сервис электронной почты» (СЭП).

ЭДО - это система (процесс) управления документами в цифровом формате, позволяющая осуществлять обмен электронной документацией внутри компании, между организациями и с госорганами. Он включает в себя создание, заверение, отправку, получение, хранение и управление электронными документами, этот формат также ориентирован на обмен электронными документами через информационно-телекоммуникационные сети или для обработки в информационных системах.

По виду электронный документооборот делят на внутренний, внешний и документооборот с госорганами.

Внутренний документооборот реализуется внутри организации. Слабо регулируется законом, поэтому каждая организация имеет право

устанавливать свои правила. Внутренний ЭДО помогает руководству и работникам организации быстро обмениваться информацией, согласовывать её и утверждать. Руководство может контролировать работу сотрудников, оценивая скорость создания, просмотра, отправки документации. Во внутреннем обороте могут быть: приказы, инструкции, справки, выписки, локальные нормативные акты и т.п.

Внешний документооборот — между организацией и её контрагентами. Документами, участвующими во внешнем электронном документообороте, могут быть договоры поставки, договоры оказания услуг, инвойсы, счета-фактуры. Такая документация обычно формируется по шаблонам, а маршруты её передвижения подчиняются отлаженным схемам.

Документооборот с госорганами реализуется между организацией и государственными структурами: пенсионным фондом, фондом социального страхования, налоговой инспекцией. Осуществлять ЭДО с госорганами помогают специальные сервисы, которые генерируют формы для документов и позволяют быстрее заполнять отчёты. В основном взаимодействие с госорганами предполагает сдачу отчётности о деятельности организации, уплату налогов, отчисления в фонды.

Для внешнего документооборота обычно выделяют 2 способа обмена: самостоятельный и через оператора ЭДО СФ. Самостоятельный обмен также называют взаимодействием «точка-точка», т. е. без посредников.

СЭП (электронная почта – «e-mail») — это «Интернет» платформа, через которую отправляются, получаются и хранятся электронные сообщения, используя специальный адрес электронной почты.

Адрес электронной почты - это уникальная строка символов, которая идентифицирует конкретного пользователя в сети Интернет. Он состоит из имени пользователя, символа «@» и доменного имени, указывающего на принадлежность к почтовому сервису (серверу). Например, ivan@yandex.ru - это адрес электронной почты пользователя по имени Иван, зарегистрированного на почтовом сервисе «Яндекс». Существует множество СЭП, таких как «Mail», «Gmail», «Yandex», «MVD» и другие, которые предоставляют пользователям удобные инструменты для обмена информацией.

Необходимо знать и понимать следующие термины:

Электронная документация — информация, которая передаётся не в бумажном, а в электронном виде. Такая документация читается, обрабатывается, передаётся не только людьми, но и машинами. При этом важно понимать разницу между понятиями «документ в электронном виде» и «электронный документ». Первый представляет собой оцифрованный бумажный носитель и является копией оригинала, а второй изначально создаётся в цифровом формате, то есть это оригинал.

Квалифицированная электронная подпись (КЭП) — это уникальная цифровая метка, принадлежащая конкретному человеку. Она накладывается

на весь конкретный документ. После этого он становится юридически значимым, а также защищённым от подделки.

Оператор ЭДО — это организация, у которой есть технические и правовые возможности обеспечивать другим организациям ведение электронной документации согласно действующим требованиям законодательства.

Контрагенты — это физические или юридические лица, государственные учреждения, с которыми у организации есть торговые, финансовые, гражданско-правовые отношения.

Для реализации внутреннего ЭДО, на рынке существует множество информационных систем, которые позволяют использовать КЭП для подписания документов. Используя такие системы, взаимодействия между своими подразделениями происходит без лишнего бумажного документооборота, а организация получает квалифицированный сервис электронного документооборота (СЭД). С такими возможностями информационные системы с ЭДО в больших организациях часто создаются и поддерживаются своими собственными силами, но в малых организациях программные продукты приобретаются отдельно.

Налаженный внутренний документооборот — это хорошо, но встает вопрос о том: «Как осуществлять внешний электронный документооборот?». Многие стали использовать обычную электронную почту для передачи корреспонденции и документов, которые прикреплялись к письму в виде электронных копий оформленных бумажных документов (с печатями и живыми подписями). Такой способ передачи документов не являлся официальным способом передачи, а лишь только показывал серьезность организаций по исполнению условий договора или это предварительная стадия согласования. В результате всё равно приходилось возить оригиналы отправленных документов для двустороннего согласования.

Появление Федерального закона от 06 апреля 2011 г. №63-ФЗ «Об электронной подписи» и иные нормативно-правовые акты определили, что теперь для отправки таких документов необходимо получить КЭП, подписать соглашение с контрагентами о переходе на ЭДО, установить сертифицированные ФСБ РФ средства криптографической защиты информации (ч. 1 ст. 6 ФЗ). Единственно, сейчас не подойдет такой способ для обмена электронными счетами-фактурами (ЭСФ), его необходимо проводить только через Операторов ЭДО. Обмен и передача некоторыми видами документов можно осуществлять без КЭП средствами электронной почты, электронные адреса которых внесены в соответствующие соглашения или договора.

Согласно всё той же ч. 1 ст. 6 Федерального закона «Об электронной подписи»: «Информация в электронной форме, подписанная КЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством РФ», за исключением некоторых случаев.

Для выполнения указанного требования нет необходимости создавать официальный бумажный документ, достаточно его создать в электронном виде, подписать всеми требуемыми лицами при помощи КЭП и отправить контрагенту. Для выполнения подписания документа КЭП, необходимо дополнительные финансовые вложения на приобретение электронных идентификаторов и СКЗИ и это необходимо делать с постоянной периодичностью.

Т.к. новые технологии постоянно развиваются, то стоимость и разновидность СКЗИ становятся доступней и применять КЭП теперь становиться проще и не так дорого. Сейчас редко встретишь организацию, в которой нет КЭП, но внешний ЭДО у них все так же происходит с использованием бумажных носителей, причем появляются новые недостатки.

Самый главный недостаток – это используя свою внутреннюю систему ЭДО (СЭД), ответственные сотрудники видят, что в ней есть нужный им подписанный КЭП документ (это визуальный графический объект на документе с указанием кто подписал его КЭП), распечатывают документ на бумажный носитель и отвозят своим контрагентам. Данный документ не является юридически значимым, т.к. этот документ является графической копией, т.е. то же самое что ксерокопия официального бумажного документа.

Поэтому в ч.1 ст.6 ФЗ «Об электронного подписи» акцентируется внимание на то, что информация в электронной форме (это фалы любых форматов, например, таких как doc, docx, xls, xlsx, pdf, jpg, avi и т.п., т.е. текстового, графического, звукового или видео форматов) должна быть подписана простой, неквалифицированной или квалифицированной электронной подписью. Для этого почти любое СКЗИ предлагает свои инструменты для осуществления подписания ЭП информации в электронной форме.

Вот другие основные недостатки использования электронной почты:

1. Отсутствует полноценный автоматизированный архив самих электронных документов с возможностью поиска. При использовании электронной почты по умолчанию бесплатно выделяется ограниченный объем для хранения писем с вложениями примерно 1 Гбайт, этого объема бывает недостаточно. Для получения дополнительного объема необходимо дополнительное финансирование. Дополнительно для писем существует ограничение на объем письма с учетом вложений, если объем письма с вложениями превышает установленный системой, то лишние вложения указываются в виде ссылок в письме, а сами они переносятся в общее облако, где они могут стать общедоступными.

2. Отсутствует автоматическая выгрузка документов. При подготовке к налоговой проверке придется выгружать по отдельности каждый документ.

3. Спам.

Все указанные недостатки ощутимы, если использовать сервисы электронной почты на постоянной основе. Для этого нужны операторы ЭДО, которые разрабатывают и согласовывают стандарты между контрагентами с

использованием своих программ или модулей интеграций в системы контрагентов.

Для эпизодических или однократных обменов с внешними контрагентами необходимо использовать почтовые клиенты и создавать структурированные папки, в которые осуществляется сортировка входящей и исходящей корреспонденции, а для борьбы со спамом использовать встроенные системы почтовых сервисов для фильтрации писем или включить фильтры, которые будут блокировать всё, кроме того, что сами укажите.

Самым важным преимуществом вижу то, что с использование КЭП, теперь существует возможность осуществлять защищенный доступ к сервисам электронной почты. С помощью встроенных инструментов СКЗИ и КЭП возможно осуществлять подписание информации в электронной форме на стороне отправителя и проверять её на подлинность на стороне получателя, тем самым уходить от расстояний и временных рамок, которые приходиться преодолевать документам в бумажном виде. Появляется возможность взаимодействия удаленно и не быть привязанным территориально для решения важных задач.

Датиев Ацамаз Аланович,
преподаватель кафедры информационной безопасности
Краснодарский университет МВД России;
Горзолия Максим Вадимович
курсант взвода 6122
Краснодарский университет МВД России

РОЛЬ ПОДРАЗДЕЛЕНИЯ ДЕЛОПРОИЗВОДСТВА В ОБЕСПЕЧЕНИИ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Совершенствование работы с документооборотом является одной из основных задач деятельности ОВД. Объем документов увеличивается, постоянно возрастает и в настоящие время особую актуальность приобретают правильная организация работы с управленческими документами, рациональное документационное обеспечение управления, систематическое совершенствование этой деятельности.

Подразделения делопроизводства в структуре Министерства Внутренних Дел всегда были и остаются ключевым звеном, они на протяжении двух веков продолжают функционировать и совершенствовать свою работу. Первая канцелярия МВД была образована 7 января 1804 года. Почему так важно обратить на это внимание? При рациональной организации делопроизводства повышается производительность, сокращаются затраты, связанные с самой деятельностью аппарата управления. Но также в системе ОВД существуют документы, имеющие защищенный доступ. Работа с таким документооборотом требует высокой ответственности, поэтому подразделения делопроизводства имеют высокую ценность. Основная цель службы делопроизводства является организация, руководство, координация и контроль документации.

Защищенный документооборот является критически важным элементом обеспечения национальной безопасности и предотвращения утечки конфиденциальной информации в органах внутренних дел. Кроме того, несанкционированный доступ к документации ОВД может привести к серьезным последствиям, включая раскрытие оперативной информации, компрометацию следствия и подрыв доверия к правоохранительным органам. В том числе, эффективный защищенный документооборот необходим для соблюдения законодательства о защите персональных данных и государственной тайны.

К методам, обеспечивающим безопасный документооборот ОВД следует отнести:

– использование электронной подписи для подтверждения целостности и подлинности документов;

– ограничение доступа к конфиденциальным документам путем установления различных уровней доступа и полномочий.

– шифрование конфиденциальных данных при передаче и хранении;

– регулярное обновление и модернизация системы защиты информации от внешних угроз;

– обучение сотрудников правилам информационной безопасности и контроль за соблюдением этих правил;

– аудит и мониторинг документооборота для выявления и предотвращения возможных нарушений;

– установление процедур и политик защиты информации, включая резервное копирование данных и контроль доступа.

– внедрение системы контроля доступа к информации с определением правил доступа для каждого сотрудника;

– разработка и внедрение регламентов и инструкций по защищенному документообороту, а также контроль за их исполнением;

– внедрение современных технологий, таких как электронный документооборот (ЭДО), системы управления документами (ECM).

Так как сервис электронного документооборота в настоящие время очень актуален и удобен в использовании. Однако, бывают случаи, когда сами владельцы недооценивают ее значимость - теряют или оставляют в общественном месте, передают другим лицам. Электронная подпись является безопасной, так как ее невозможно подделать, ведь при ее создании подразделения делопроизводства используют криптографические методы шифрования. Чтобы использовать электронную подпись, потребуется установить специальное приложение, обеспечивающее защиту информации.

Если же рассматривать организационно-правовую составляющую роли подразделений делопроизводства в обеспечении защищенного документооборота, то нельзя не упомянуть о том, что происходят постоянные изменения в законодательстве о защите информации и персональных данных, которые требуют оперативного обновления внутренних регламентов и инструкций. В том числе появление новых отечественных форматов документов вносит необходимость работы с большими объемами данных при адаптации существующих систем и процессов.

В заключение следует отметить, что подразделение делопроизводства играет критическую роль в обеспечении защищенного документооборота в органах внутренних дел. Эффективная работа этого подразделения напрямую влияет на национальную безопасность, предотвращение утечек конфиденциальной информации и соблюдение законодательства. Современные вызовы, связанные с ростом объемов документооборота, переходом на электронные технологии и усилением киберугроз, требуют постоянного совершенствования системы защищенного документооборота. Необходимо инве-

стировать в модернизацию информационных систем, повышать квалификацию сотрудников подразделений делопроизводства, внедрять современные методы обеспечения информационной безопасности и оптимизировать рабочие процессы. Дальнейшие исследования должны быть направлены на разработку более совершенных методов защиты информации и оптимизацию рабочих процессов с учетом специфики деятельности органов внутренних дел.

Литература

1. Заботина, Т. Ю. Роль подразделений делопроизводства и режима в повышении качества подготовки документов и обеспечения контроля за документационным обеспечением в ОВД / Т. Ю. Заботина // Гуманитарные научные исследования. – 2015. – № 5-2(45). – С. 42-44. – EDN TZVHWP.

2. Краснов, М. С. Организация защиты служебной информации и персональных данных на примере отдела образования / М. С. Краснов, М. Ю. Козлов, Н. В. Седова // Психолого-педагогический журнал Гаудеамус. – 2011. – Т. 2, № 18. – С. 104-106. – EDN OCPOEP.

Датиев Ацамаз Аланович,
преподаватель кафедры информационной безопасности
Краснодарский университет МВД России;
Дзагкоев Сослан Русланович
курсант взвода 6122
Краснодарский университет МВД России

ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА В ДЕЛОПРОИЗВОДСТВЕ

В современном мире информационные технологии играют ключевую роль в деятельности органов внутренних дел. Эффективное делопроизводство в этой сфере требует не только высококачественного программного обеспечения, но и надежной аппаратной защиты. Необходимо обозначить важность программно-аппаратной защиты в делопроизводстве ОВД, в том числе основные методы обеспечения безопасности.

Программно-аппаратная защита в делопроизводстве ОВД включает в себя применение технических инструментов и специализированных сервисов, направленных на защиту конфиденциальных данных.

Рассмотрим некоторые из них:

1) ИСОД представляет собой интегрированную информационную сеть, которая связывает различные структуры внутри МВД и способствует сотрудничеству с внешними организациями. В рамках этой сети функционирует множество сервисных функций, каждая из которых выполняет уникальные задачи. Особенно значимым является Сервис Управления Доступом к Информационным Системам и Ресурсам (СУДИС). Данная система обеспечивает процесс идентификации пользователей, позволяя определять, кто имеет доступ к системе и ее ресурсам. Это включает в себя использование паролей, биометрических данных или других методов аутентификации. После идентификации СУДИС управляет правами доступа пользователей к различным системам и сервисам ИСОД. Это значит, что каждый пользователь получает доступ только к тем функциям, которые необходимы для выполнения его служебных обязанностей. Так же сервис управления доступом к информационным системам и ресурсам ведет журнал действий пользователей, что позволяет отслеживать, кто и когда получал доступ к определенным данными. Это важная возможность для обеспечения безопасности и выявления возможных нарушений. СУДИС может использовать методы шифрования для защиты данных, передаваемых между пользователями и системой, что обеспечивает дополнительный уровень безопасности.

2) RuToken представляет собой компактный электронный идентификатор, выполненный в формате USB-брелка. Он предназначен для безопасной аутентификации и хранения конфиденциальной информации. Это утройство ялвяется отличной альтернативой сложным системам паролей,

поскольку не требует запоминания трудных комбинаций. Все пароли хранятся непосредственно в самом устройстве. Для выполнения аутентификации пользователю необходимо подключить RuToken к USB-порту и ввести короткий PIN-код. RuToken предоставляет возможность хранения электронной подписи сотрудника МВД на персональном идентификаторе, что существенно облегчает процесс подписания документов и взаимодействия с электронными системами. Электронная подпись, размещенная на RuToken, обладает юридической значимостью и гарантирует высокий уровень защиты данных, что имеет особое значение для делопроизводства. Одним из основных преимуществ RuToken является возможность доступа к системе и сервисам ИСОД МВД России без необходимого повторного ввода логина и пароля. Это не только упрощает процесс аутентификации, но и минимизирует риск ошибок, связанных с вводом учетных данных. Сотрудник подключает RuToken к компьютеру, после чего система автоматически идентифицирует его, обеспечивая быстрый и безопасный доступ к нужным ресурсам. Еще одним преимуществом RuToken является автоматическая блокировка рабочего места при извлечении идентификатора, то есть как только сотрудник вынимает токен из порта, доступ к его рабочему месту автоматически закрывается. Эта мера защищает информацию от несанкционированного доступа в случае, если сотрудник временно покинул свое место или забыл завершить сеанс.

3) В дополнение к RuToken, важным компонентом системы аутентификации и работы с электронными документами в делопроизводстве МВД РФ является программный продукт “КриптоПро” он предоставляет возможность использования электронной подписи при взаимодействии с сервисами ИСОД, что существенно упрощает и ускоряет процессы документооборота и идентификации пользователей. Система гарантирует надеждную идентификацию пользователей с использованием их электронной подписи. Это дает возможность оперативно проверить подлинность подписей и убедиться, что документ был подписан именно уполномоченным лицом, что значительно снижает риски мошенничества и несанкционированного доступа. Применение электронной подписи вместе с высокими стандартами криптографической защиты данных гарантирует надежную защиту информации и снижает риски утечки или фальсификации документов. КриптоПро представляет собой ключевое дополнение к системе RuToken и другим инструментам, применяемым в МВД РФ для повышения безопасности и эффективности делопроизводства.

4) Антивирусное внедрение: периодическое обновление антивирусных приложений и применение систем для выявления вторжений способствуют предотвращению атак и утечек данных. С целью снижения рисков проникновения вредоносного кода в информационные системы в рамках программы обеспечения информационной безопасности (ПОИБ) ИСОД

МВД России была разработана инновационная технологическая инфраструктура антивирусной защиты, основанная на антивирусе Касперского. На сегодняшний день эта система не имеет аналогов в стране по своему масштабу. К ней подключены автоматизированные рабочие места пользователей и серверное оборудование. Антивирус Касперского обеспечивает защиту от вредоносного ПО и почтового спама, сохраняет целостность данных, позволяет проводить инвентаризацию программного и аппаратного обеспечения, а также контролировать использование внешних съемных устройств.

Таким образом, проведя обзор существующих программных и аппаратных средств безопасного хранения, обработки и передачи информации при решении задач делопроизводства, становится ясно, что необходимо использовать комплексный подход. Приведенные программно-аппаратные средства обеспечат достаточной защищенностью. Но не стоит забывать, что вредоносные программы активно развиваются, поэтому необходимо внимательно следить за тенденциями IT-технологий и своевременно создавать новые инструменты обеспечения безопасного делопроизводства.

Назаров Артур Карапетович,
кандидат технических наук
старший преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

КРИПТОГРАФИЯ: СОВРЕМЕННЫЕ АЛГОРИТМЫ И ЕЕ БУДУЩЕЕ

Алгоритмы шифрования давно применятся не только военными и дипломатами для защиты конфиденциальной информации, но людьми, которые желают скрыть свои сообщения от посторонних. На сегодняшний день использование криптографии – это неотъемлемая часть современного цифрового мира. Это достигается в первую очередь потому, что современные шифры имеют высокий уровень криптостойкости. К таким алгоритмам, можно отнести, например, следующие: симметричный алгоритм блочного шифрования AES-256 (Advanced Encryption Standart), ГОСТ 34.12-2018, ECC (Elliptic-Curve Cryptography) и др. Алгоритм AES-256 используется, к примеру, для шифрования данных облачными сервисами Google Drive, DropBox, OneDrive.

Применение современных алгоритмов шифрования обосновано не только для задач, связанных с сокрытием передаваемых или хранимых сообщений. Так, ассиметричная криптография широко используется для обмена ключами, цифровых подписей и т.д. К примеру, алгоритмы RSA или ECC используются для обмена ключами облачными сервисами Google Drive, DropBox, OneDrive. ECC также применяется в стандартах мобильной связи 5G для обеспечения аутентификации и защиты данных. Другим примером использования является технология блокчейн: криптовалюты Bitcoin и Ethereum – использует ECC для создания и проверки цифровых подписей транзакций. Также ECC может встречаться в IoT (интернет-вещей) для обеспечения безопасности данных.

Отдельно стоит упомянуть криптографические хеш-фнкции – алгоритмы преобразующие данные произвольного размера в некоторый фиксированный массив данных, определенной длины. Этот массив часто называют еще хешем, дайджестом или «отпечатком пальца». Среди семейства современных безопасных хеш-функций особое место занимают SHA (Secure Hash Algorithm): SHA-1, SHA-256 и др.

Криптография защищает наши финансовые данные при доступе к онлайн услугам банков (например, при совершений покупок в интернете). При этом используются протоколы SSL/TLS для обеспечения безопасности интернет соединений (например, на сайтах, использующих протокол https://).

В приложениях для мгновенного обмена сообщениями создается шифрованный тоннель для передачи данных с помощью сквозного шифрования. Этот алгоритм позволяет обеспечивать приватность передаваемых сообщений.

Не смотря на кажущуюся надежность современных шифров, они не обеспечивают стопроцентной защиты. Развитие информационных технологий может привести к уязвимости некоторых из них в будущем. Например, возможное появление в будущем квантовых компьютеров, обладающих высокой скоростью вычислений, может привести к революции в области вычислений и является потенциальной угрозой для многих современных криптосистем. Это связано с тем, что большинство алгоритмов шифрования, используемых в настоящее время (например, RSA, ECC), основываются на решении сложных математических задач, но квантовые компьютеры, благодаря своим особенностям, могут эффективно решать подобные задачи при помощи соответствующих алгоритмов. К примеру, известный алгоритм Шора позволяет решить задачу факторизации больших чисел за экспоненциальное время, что, в свою очередь, ставит под угрозу использование алгоритма RSA.

Другой угрозой может стать развитие искусственного интеллекта, который может быть интегрирован с другими системами, применяемыми для взлома криптоалгоритмов.

В связи с этим в настоящее время ведутся исследования в области постквантовой криптографии –разрабатываются алгоритмы, независимые от квантовых вычислений, то есть устойчивых к квантовым атакам. Среди таких алгоритмов можно выделить, например:

Lattice-based cryptography (криптография на основе решёток) – подход к построению алгоритмов асимметричного шифрования с использованием задач теории решёток, то есть задач оптимизации на дискретных аддитивных подгруппах, заданных на n-мерном множестве вещественных чисел.

Multivariate cryptography (многомерная криптография) – асимметричные криптографические схемы, построенные на решениях уравнений, основанных на многомерных полиномах над конечным полем.

Hash-based cryptography (криптография на основе хэша) – криптографические примитивы, основанные на безопасности хеш-функций.

Code-based cryptography (криптография на основе кода) – криптографические системы, основанные на кодах с исправлением ошибок.

Isogeny-based cryptography (криптография, основанная на изогении) – это криптографические системы, основанные на свойствах изогенных графов эллиптических кривых.

Symmetric key quantum resistance (квантовое сопротивление симметричного ключа) – при условии использования достаточно больших размеров ключей криптографические системы с симметричным ключом, такие как AES и др., уже устойчивы к атакам с использованием квантового компьютера.

К примеру, новыми стандартами постквантовой криптографии являются Kyber, NTRU, FrodoKEM.

Таким образом, криптография продолжает как и ранее обеспечивать защиту данных, не смотря на растущие потенциальные угрозы, и успешно справляется с новыми вызовами. Исследования, проводимые сегодня в сфере постквантовой криптографии, вероятнее всего в будущем станут основой безопасности данных.

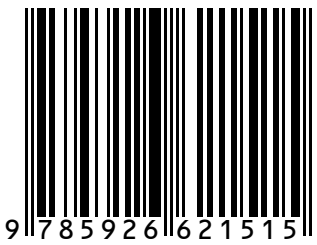
Научное издание

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ДЕЛОПРОИЗВОДСТВА И РЕЖИМА

Материалы
Всероссийской научно-практической конференции
(23 октября 2024 г.)

В авторской редакции

ISBN 978-5-9266-2151-5



Подписано в печать 10.02.2025.
Авт. л. 2,8. Заказ 323.

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