Министерство науки и высшего образования РФ
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«Тверской государственный университет»
Юридический факультет
Кафедра судебной власти и правоохранительной деятельности
Направление подготовки
40.03.01 ЮРИСПРУДЕНЦИЯ
Профиль «Правопользование и правоприменение»

КУРСОВАЯ РАБОТА
По дисциплине Правоохранительные органы
на тему:

Правовые основы деятельности правоохранительных органов по обеспечению информационной безопасности.

Выполнила: студентка 1 курса 13 гр.
Рябчикова Ульяна Максимовна

Научный руководитель: к.ю.н, доцент
Замрий Олег Николаевич

Тверь 2020

СОДЕРЖАНИЕ

Введение

В настоящее время всё быстрее и быстрее происходит развитие информационных технологий, которые проникли в каждую сферу нашей жизни. Несомненно, использование достижений научно-технического прогресса во многих аспектах упростила жизнь людей, глобально расширило информационное пространство, однако всё это в свою очередь повлекло за собой появление новых угроз в информационной сфере.

Актуальность темы обусловлена тем, что технологии стали неотъемлемой частью каждого из нас, соответственно каждый находится под угрозой преступлений, связанных с информационной безопасностью. Киберпреступность является относительно новым явлением в нашей жизни, что осложняет работу правоохранительных органов, так как существует проблема недостаточной осведомленности в сфере информационных технологий. Правильная, наиболее целесообразная организация работы органов, без которой немыслима эффективная борьба с преступностью – важный вопрос современного мира.

Одной из главных задач является борьба с такого рода преступлениями. Разрешение данной проблемы связано с эффективностью работы правоохранительных органов, их целостности, а также повышения их уровня познания в информационно-телекоммуникационных технологиях. Сегодня перед сотрудниками органов стоит приоритетные задачи, в числе которых повышение качества расследования, пресечение данных угроз. Именно поэтому эта тема является актуальной в наши дни.

Целью исследования является анализ основ деятельности правоохранительных органов в области информационной безопасности, изучение теоретических и практических проблем правового регулирования и правоприменительной практики правоохранительных органов по данному вопросу.

В соответствии с поставленной целью задачами являются:

1. Проанализировать основания и порядок, полномочия органов государственной власти в сфере информационной безопасности

2. Исследовать правовые основы деятельности правоохранительных органов по обеспечению информационной безопасности

3. Проанализировать правоприменительную (судебную практику) по вопросу применения законодательства в области информационной безопасности

4. Сформулировать предложения по совершенствованию (модернизации, изменению) законодательства по вопросу информационной безопасности

Глава 1. Правовое регулирование обеспечения информационной безопасности РФ

Регулирование общественных отношений-задача не только государства, но и правоохранительных органов. Законодательство в сфере информационной безопасности появилось не так давно как в России, так и во всем мире. Конечно же, это связано со стремительным развитием компьютерных технологий. В связи с этим появилась необходимость урегулирования различных отношений, которые возникают в сети Интернет, ликвидации угроз объектам информационной безопасности и минимизация ущерба, который может быть нанесен впоследствии осуществления данных угроз. Для всего этого необходимо введение различных нормативных актов, которые, несомненно, помогают в решении проблемы. В законодательстве даже закреплена классификация сведений, безопасность которых необходимо обеспечить:

1. Сведения, отнесенные к государственной тайне. Определение данных сведений изложено в ст.5 Закона РФ «О государственной тайне»[1] - это информация в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации.

2. Сведения, отнесенные к коммерческой тайне, защита которых регламентирована ст.5 Федерального закона "О коммерческой тайне"[2] и под такими сведениями понимается информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, если к ней нет законного доступа на законных (санкционированных)

[1] Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1
[2] Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

основаниях и обладатель такой информации принимает меры к охране ее конфиденциальности.

3. Сведения, имеющие статус персональных данных, под которыми, в соответствии со ст.3 Федерального закона "О персональных данных"[1] понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). "

Для начала необходимо упомянуть такой законодательный акт, как Федеральный закон от 28.12.2010 № 390-ЦЗ "О безопасности"[2]. Он закрепляет правовую основу безопасности личности в целом, не только в сфере информационных технологий, однако тем самым он не становится менее важным, ведь в нем так же прописан порядок организации правоохранительных органов, их финансирование и так далее.

Изначально в Российской Федерации с 1995 по 2006 года действовал Федеральный закон РФ «Об информации, информатизации и защите информации»[3], который являлся законодательным актом, регулирующим отношения общества в сфере информационных технологий, бравший своё правовое начало из Конституции. Он закрепил обязательность документирования информации, установил ряд терминов, урегулировал отношения, возникающие при создании и использовании информационных технологий, установил обязанность предоставления информации государственным органам. Данный акт включал в себя такие главы, как информационные ресурсы как элемент состава имущества и объект права собственности, пользование информационными ресурсами, защита информации и прав субъектов в области информационных процессов и информатизации. Так же, что является не мало важным, в документе чётко

[1] Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
[2] Федеральный закон "О безопасности" от 28.12.2010 N 390-ФЗ
[3] Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"

прописывалась классификация информационных ресурсов (открытая общедоступная информация, конфиденциальная информация, персональные данные о гражданах и тд), что даёт людям понять всё различие информации, которая им предоставлена.

Однако информационный прогресс шёл слишком быстро и данный акт устарел. Тогда его заменили на Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»[1], который был принят в 2006 году и действует по сей день. Так же данный закон стал объектом исследования Инюшкина Андрея Алексеевича. Автор в своей статье[2] рассмотрел некоторые особенности документа, его достоинства, однако, в ходе анализа он нашел и недостатки (например, определении баз данных отсутствуют иные термины, охватывающие правовую характеристику информации, изложенной в ст. 2 Фз «Об информации», а именно -«сведения», «сообщения» и «данные». Вместо них в легальном определении баз данных использован термин «материалы» и приводится открытый перечень конкретных примеров). Несмотря на то, что в акте присутствуют какие –то минусы, он всё –таки был создан для следующих целей:

1.Устранения пробелов в теоретической части, введение понятий (приведение в порядок понятийного аппарата)

2.Необходимость создания правовой основы, которая реализовала бы право граждан на защиту в информационное сфере

3.Точное закрепление подходов регулирования отношений, возникающих в сфере информационных технологий

Данный документ взял за основу содержание прошлого акта, но существенно дополнил его.

[1] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

[2] Инюшкин А.А. Особенности применения Федерального закона от 27. 07. 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Право. 2017

Далее рассмотрим статью Мысева Алексея Эдуардовича и Морозова Николая Владимировича «Правовое регулирование информационной безопасности в Российской Федерации»[1]. В данной публикации они обращают своё внимание на историю развития Российского законодательства в сфере информационных технологий. Мысевым и Морозовым были проанализированы различные нормативно правовые акты, одними из которых являются Доктрины 2000 года и 2006 года. Они сравнивают эти две Доктрины. Однако далее мы рассмотрим особенности каждого из этих документов.

Итак, Доктрина информационной безопасности Российской Федерации 2000 года[2]. Как отмечается в преамбуле документа, правовую основу Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации. Согласно данному акту информационная безопасность-состояние защищенности национальных интересов Российской Федерации, которой посвящена первая глава (национальные интересы, источники угроз информационной безопасности). Интересы государства в информационной сфере заключаются в создании условий для развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области предоставления информации и пользования ею в целях обеспечения незыблемости конституционного строя, территориальной целостности, суверенитета, в безусловном обеспечении законности и правопорядка, развитии взаимовыгодного и равноправного международного сотрудничества.

[1] Мысев А.Э.; Н.В. М Правовое регулирование информационной безопасности в Российской Федерации // Право 2019

[2] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)

Так же Доктрина включает в себя Четыре основные составляющие национальных интересов РФ в информационной сфере:

1.Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею

2.Информационное обеспечение государственной политики РФ

3.Развитие современных информационных технологий

4.Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных сетей

Помимо национальных интересов в Доктрине закреплены общие методы обеспечения информационной безопасности страны, которые в свою очередь подразделяются на:

1.Правовые

2.Организационно-технические

3.Экономические

Доктрина внесла большой вклад в формирование правового регулирования обеспечения информационной безопасности РФ

Доктрина 2000 года действовала достаточно долгое время, вплоть до 2016, когда ее отменили из-за утверждения новой Доктрины[1], которая по своей сути отличается от неё. В новом акте под информационной безопасностью понимается «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”

информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений». Нельзя не подметить то, что в Доктрине закреплены основные используемые понятия, которые выделили в отдельные пункты. Данный факт не может не радовать, так как таким образом люди могут лучше разобраться в документе без помощи профессионалов и различных специалистов. Еще одним нововведением является более чёткая и современная установка задач правоохранительных органов:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.»

Доктрина 2016 года также, как и Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» действует в настоящее время и входит в систему правового регулирования обеспечения информационной безопасности.

Таким образом, рассмотрев Доктрины с точки зрения законодательства и с точки зрения авторов научной статьи, можно сделать вывод о том, что эти

документы, несомненно, внесли большой вклад в правовое обеспечение информационной безопасности. Так же Морозов и Мысев отмечают, что Доктрина 2006 года является документом, который основан на Доктрине 2000 года: «Доктрина информационной безопасности РФ продолжает курс, который был задан предыдущей версией документа, но при этом учитываются изменения, которые происходят в сфере информационных технологий». Это говорит нам о том, что законодательство понимает, что сфера информационных технологий быстро развивается, влеча за собой появление различных угроз, и пытается как-то усовершенствовать действующие законы, не забывая об основах.

Далее был принят Указ Президента Российской Федерации «О некоторых вопросах информационной безопасности Российской Федерации»[1]. были осуществлены следующие действенные мероприятия:

1) сегмент международной информационной сети, применяемый органами законодательной, судебной и исполнительной власти, преобразован в российский государственный сегмент этой сети;

2) закреплен единый порядок подключения информационных систем и информационно-телекоммуникационных сетей к Интернету и опубликования в ней информации через этот сегмент, предусматривающий ее передачу по каналам связи, защищенным с внедрением криптографических средств.

Наконец, хочу обратить внимание на 152-Федеральный Закон «О персональных данных», который регулирует отношения с данными. Закон возлагает обязанности на тех, кто хранит и собирает эти данные. Целью данного Федерального закона, как и остальных, обозначается обеспечение прав и свобод граждан в сфере информационных технологий. Ключевыми

[1] Указ Президента РФ от 22 мая 2015 г. N 260 "О некоторых вопросах информационной безопасности Российской Федерации"

моментами являются принципы и условия обработки информации, из которых основные:

1.Необходимо согласие владельца персональных данных перед их сбором и обработкой

2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.Если владелец персональных данных обратиться с просьбой удалить их, вы будите обязаны сделать это

4.Обработка и хранение персональных данных должна осуществляться на территории Российской Федерации

Данный документ очень важен для обеспечения информационной безопасности, ведь персональные данные это сведения о лице, которые, попав в руки мошенников, могут привести к неблагоприятным последствиям.

В данной главе я рассмотрела, на мой взгляд, основные документы, которые входят в систему правового регулирования информационной безопасности. Так же существуют и другие акты, которые помогают регулировать отношения в этой огромной информационной площадке. К ним относятся:

1. 63-ФЗ «Об электронной подписи»[1] (определяет правовой режим технологического обеспечивания обороны информации в системе базисных законов информационного законодательства

2. 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2]

3. Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ.

[1] Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ
[2] Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

4. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона[1]"О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных" и федерального закона "О персональных данных"

5. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[2]

6. Международные конвенции об охране информационной собственности, промышленной собственности и авторском праве защиты информации в Интернете;

7. Положение о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов РФ.

Однако, не смотря на достаточно неплохую правовую базу, в настоящее время растет преступность, связанная с информационными технологиями. Совершенствование должно, как мне кажется, происходить не только в законодательстве, но и в деятельности правоохранительных органов, которые обеспечивают своими действиями информационную безопасность.

[1] Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О специальной оценке условий труда" от 28.12.2013 N 421-ФЗ
[2] Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"

Глава 2. Организационно-правовые основы деятельности правоохранительных органов в сфере обеспечения информационной безопасности

С развитием науки информационные технологии стали инструментом различных преступлений, связанных с информационными технологиями. С помощью Интернета происходит уничтожение данных, «выброс» компрометирующей информации, а также другие нарушения, которые представляют угрозу для общества и государства. К примеру, обезналичивание платежей, которое активно производится преступниками, является большой проблемой, так как средства народа и государства находятся под ударом. Так по обнародованным данным Генерального прокурора мы можем понять, что за 2019 год число преступлений в информационной сфере увеличилось более чем в полтора раза, что на 66,8% больше, чем в том году. Данные сведения заставляют органы защиты задуматься над тем, какие же действия им необходимо предпринять, чтобы сократить преступность с использованием информационно-телекоммуникационных технологий.

В данном аспекте можно обратится к научной статье А.В. Аносова «Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий»[1], в которой он рассматривает проблему информационной преступности и показывает нам ,исходя из общих задач правоохранительных органов по предупреждению и пресечению киберпреступлений на какие комплексы мер было обращено внимание:

1. Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий. В научном сообществе преобладает такая точка зрения, в которой основной целью предупреждения преступлений в сфере информационных технологий

[1] Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Право. 2018

определяют формирование конкретных правил использования информации, максимально ограничивающих условия и возможности незаконного воздействия на нее. Главным итогом научной работы должен являться адаптированный перенос ее итогов в правоприменительную практику. Координирование усилий органов защиты должно осуществляться уже на этапе сбора криминологической информации и далее представлять собой особую систему , которая позволяет беспрепятственно обмениваться информацией в процессе предупреждения, раскрытия и расследования информационных преступлений.

2. Усовершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями в сфере высоких технологий. Данный пункт предполагает совершенствование подзаконных актов и документации, которая способствует обеспечению информационной безопасности и пресечению преступлений

К отдельным тенденциям совершенствования научно-методического обеспечения противодействия высокотехнологичной преступности относятся:

1)унификация терминов, связанных с высокими технологиями, ведь понятие «информационные технологии» может включать в себя не только преступления, которые предусмотрены в главе 28 УК РФ, в которой информационные технологии представлены средством совершения преступления. Объект состава преступления часто включает в себя также и другие общественные отношения, мошенничество с помощью компьютерных технологий, сбыт наркотических и психотропных средств, используя электронную сеть и тп.

2) формирование правовых механизмов, сужающих пространство для совершения противоправных деяний. В данном пункте предполагается на законодательном уровне закрепить обязанность продавцов техники устанавливать антивирус, а также заключать с покупателем страховой

договор. Такие процедуры направлены на снижение количества несанкционируемых проникновений

3) разработка новых прикладных методик противодействия компьютерной преступности, в том числе в процессе оперативно-розыскной профилактикиПо данному предложению предполагается законодательное закрепление полномочий на осуществление проверки опубликованных в сети Интернет материалов, которые могут содержать экстремистские или подобные идеи

3. Принятие организационно-управленческих мер предупреждения высокотехнологичных преступлений.

К данным мерам относятся:

1)подготовка правоохранительных органов по специальностям, которые направлены на обеспечение информационной безопасности в таких образовательных учреждениях, как МВД, ФСБ, МО, ФТС России и др

2) переход от преимущественно территориального принципа работы правоохранительных органов в сфере предупреждения преступлений к функциональному. Зачастую трудно определить место преступления, а значит трудно определить, какой территориальный орган будет заниматься расследованием, поэтому необходимо специализировать деятельность органов не только на региональном уровне, но и на районном.

3) перевод на новый уровень организацию взаимодействия правоохранительных органов со средствами массовой информации. Данное взаимодействие должно характеризоваться отчётом правоохранительных органов перед народом, распространении пропаганды, которая формировала бы в сознании общества нетерпимость к информационным преступлениям, а также, выкладывая информацию о мерах защиты, повышать информационную культуру населения.

Таким образом, Аносов подводит нас к выводу о том, что использование различных мер предупреждения преступлений повышает уровень информационной безопасности в стране. Так же из его стати можно понять, что, конечно, правоохранительным органам есть куда расти в сфере информационных технологий, однако, используя различные средства, есть возможность достижения цели.

Далее хочу отметить, что, так как деятельность правоохранительных органов связана с сетью Интернет, им необходимо непосредственное взаимодействие с различными инновационными технологиями, внедрение их в работу. Таким образом такое внедрение усовершенствует систему расследования преступлений.

Так правоохранительные органы активно применяют устройство «Терминал –ТМ-5», которое выполняет информационную функцию (с помощью нее происходит выявление лиц, находящихся в федеральном и местном розыске). Также хорошими помощником в поиске необходимых лиц являются «Гастролеры» и АИСС «Картотека-Регион». Нельзя не отметить значимость таких АИПС, как «Автопоиск», «Банкир», «Вещь», «Маньяк» и др.

Ключевую роль в повышении уровня информатизации работы правоохранительных органов сыграл Главный информационно-аналитический центр МВД России, который внедрил криминальный учёт- это специально систематизированные информационные данные о фактах, лицах и тп, которые предназначены для более эффективного информационного обеспечения оперативно-розыскной деятельности. Исходя из данных, раскрываемость преступлений после внедрения различных информационных систем по отношению к суммарному показателю раскрытых преступлений с 2000 года по 2018 год вырос с 43% до 80%. Данный показатель даёт нам понять, что деятельность правоохранительных органов по вводу в их систему различных программ, устройств и тп, которые направлены на повышение

качества работы, действительно помогла добиться успехов в информационной безопасности.

Особую роль в развитии информационных ресурсов и информационных систем занимают: утверждение достаточно развитой системы информационной поддержки деятельности органов власти и местного самоуправления; создание единой системы нормативно-правовых баз данных в составе информационно-правового пространства России (ведь в данном аспекте необходимо, чтобы в организации работы правоохранительных органов происходило внедрение различных информационных технологий, использование которых поставило бы сотрудников на один уровень с киберпеступниками, которые профессионально используют их) Одним из тех, кто занимается данными мероприятиями, является Министерство Юстиции РФ. Орган исполнительной власти занимается обеспечением информатизации регионов и следит за развитием законодательства субъектов РФ. Еженедельно из Министерства Юстиции РФ в регионы направляются различные нормативные акты, издаваемые различными законодательными органами.

Помимо согласования и контроля развития правового массива РФ Министерство юстиции РФ производит учёт различных нормативных правовых актов РФ, а также имеет достаточно развитую систему правовой информации и принимает участие в процессах информатизации правоой системы РФ. Основным информационным ресурсом являются различные базы данных правовых актов. Вообще, в системе правовой информации Министерства юстиции РФ особое место принадлежит информационным ресурсам судебной практики и правовой статистики, данные, которых во многом отражают результативность функционирования всей правоохранительной системы и позволяют законодателю работать с оперативной информацией и вести информационно-аналитические исследования состояния правопорядка с тем, чтобы обеспечить адекватное

правовое регулирование либо оценить эффективность существующего правового регулирования в данной области.

В целях удовлетворения информационных потребностей органов государственной власти (равно и других субъектов правовой системы) Министерством юстиции РФ был проведен анализ существующих глобальных справочных систем по законодательству, в результате которого была выделена Общемировая информационно-правовая сеть (Global Legal Information Network – GLIN), функционирующая на базе Библиотеки Конгресса США.

Ещё одним необходимым направлением работы Министерства юстиции РФ в области информационно-правового обеспечивания субъектов правовой системы считаются налаживание интернационального информационного обмена и роль информационного ресурса Министерства юстиции РФ в интернациональных системах правовой инфы. Одной из этих систем считается информационно-правовое пространство Содружества Независящих Стран, которое основывается на основании Концепции, утвержденной заключением Совета глав правительств от 18 октября 1996.

Информационные технологии Прокуратуры РФ

В рамках Программы правовой информатизации РФ в НИИ задач закрепления законности и правопорядка при Генеральной прокуратуре РФ на базе методологии системного структурного анализа разработана так же Концепция сотворения автоматической системы информационного обеспечивания органов прокуратуры Российской Федерации (АСИО-Прокуратура). Единая информационная среда создается для органов прокуратуры, распределенных по всей территории России и образующих трехуровневую систему: 1 уровень – Генеральная прокуратура РФ; 2 уровень – прокуратуры республик в составе Российской Федерации; прокуратуры краев, областей, городов Москвы и Санкт-Петербурга, автономной области, автономных округов; иные территориальные прокуратуры;

специализированные прокуратуры, приравненные к прокуратурам областей; 3 уровень – прокуратуры городов и районов; специализированные прокуратуры, приравненные к прокуратурам районов.

На региональном уровне действуют:

- АСИО «Надзор за следствием и дознанием», включающая подсистемы обработки информации по уголовным делам с продленными сроками следствия и содержания обвиняемых под стражей, по делам о преступлениях, совершенных организованными группами;

- АСИО о кадровом составе органов прокуратуры, где существует персональный учет кадров, контроль за проведением аттестации сотрудников прокуратуры и реализацией результатов ее проведения;

- автоматизированная система обработки статистически информации о работе прокурора, отчета о следственной работе, о рассмотрении заявлений и сообщений о преступлениях;

- автоматизированные системы информационного обеспечения расследования преступлений и так далее.

Компьютерная база органов прокуратуры сосредоточена в основном на центральном и областном уровнях. В последнее время персональные ЭВМ стали устанавливаться также в районных и городских прокуратурах.

Так же существует еще один элемент, который помогает организации правоохранительных органов в сфере информационной безопасности- это Главный информационный центр – наиболее крупный банк оперативно-справочной и розыскной информации в системе МВД России. Его задачей является обеспечение органов и учреждений внутренних дел информацией – статистической, криминалистической, производственно-экономической, научно-технической и так далее. Информационные центры МВД, УВД считаются важнейшим элементом информационного ОВД РФ. На

них возложена огромная нагрузка-обеспечение информационной поддержки ОВД в розыске преступников, раскрытии преступлений и так далее.

Заключение

Таким образом можно сделать следующие выводы. Преступления в сфере информационных технологий-это сложная проблема. С развитием компьютерных технологий растёт уровень преступности, а значит увеличивается риск того, что будут нарушены права граждан в информационном пространстве. По данным о состоянии преступности за 7 месяцев 2020 года, которые были опубликованы МВД, мы можем наблюдать незначительный рост общего количества зарегистрированных в стране преступлений на 0,5%, но это в основном связано с киберпреступностью. Число преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на 94,6 процента, в том числе тяжких и особо тяжких - на 129,7 процента. При этом расчетные карты использовались в криминальных целях почти в 6 раз чаще, чем годом раньше, а средства мобильной связи - более чем в 2 раза чаще. Из предоставленных данных, можно судить о том, насколько преступники проникли в сеть Интернет, совершая там всякого рода нарушения.

Необходимо сказать, что информационная безопасность определяется способностью нейтрализовать воздействие по отношению к опасным, ущемляющим интересы страны информационным воздействиям на уровне, как внедрения, так и извлечения информации.

Исходя из вышесказанного, можно отметить то, что правоохранительным органам стоит обратить особое внимание на улучшение эффективности работы в сфере информационной безопасности (повышать квалификацию в этом вопросе, внедрять в систему больше технологий, сотрудничать с организациями, которые предоставляют услуги в информационной сфере), ведь от этого зависит уровень информационной безопасности как населения, так и государства.

Список используемой литературы

Нормативно –правовые акты:

1. . Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”

2.Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"

3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

4. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)

Специальная литература:

1.Авдеева Е.В., В.А. Гордеева Оптимизация деятельности правоохранительных органов в контексте внедрения информационно-коммуникационных технологий // Закон и право. 2018 URL: file:///C:/Users/User/Downloads/optimizatsiya-deyatelnosti-pravoohranitelnyh-organov-v-kontekste-vnedreniya-informatsionnokommunikatsionnyh-tehnologiy.pdf

2. Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Право. 2018 URL: https://cyberleninka.ru/article/n/spetsialno-kriminologicheskoe-preduprezhdenie-prestupleniy-sovershaemyh-s-ispolzovaniem-vysokih-tehnologiy

3. Бецков А.В. О некоторых аспектах правового обеспечения информационной безопасности // Право. 2018г. https://cyberleninka.ru/article/n/o-nekotoryh-aspektah-pravovogo-obespecheniya-informatsionnoy-bezopasnosti-1/viewer

4. Инюшкин А.А. Особенности применения Федерального закона от 27. 07. 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

информации» // Право. 2017 URL: https://cyberleninka.ru/article/n/osobennosti-primeneniya-federalnogo-zakona-ot-27-07-2006-149-fz-ob-informatsii-informatsionnyh-tehnologiyah-i-o-zaschite-informatsii-k

5. Мустакимов Р.М. Проблемы расследования преступлений в сфере информационной безопасности // Право. 2020 https://cyberleninka.ru/article/n/problemy-rassledovaniya-prestupleniy-v-sfere-informatsionnoy-bezopasnosti

6. Мысев А.Э.; Н.В. М Правовое регулирование информационной безопасности в Российской Федерации // Право 2019 URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-informatsionnoy-bezopasnosti-v-rossiyskoy-federatsii

Дата 09.12.20 Подпись