СПЕЦИАЛЬНЫЕ КРИТЕРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНА ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

Савченко О. А.[1]

Объектом настоящего исследования является информационная безопасность органа предварительного расследования как участника информационных правоотношений. Предмет исследования представляет собой модель специальных критериев безопасности информационных технологий, применяемых органом предварительного расследования. Актуальность темы исследования обусловлена необходимостью обеспечения информационной безопасности органов предварительного расследования в процессе осуществления их полномочий. Целью исследования является разработка критериев информационной безопасности отдельного участника информационных правоотношений, дополняющих предусмотренные международными правовыми актами и действующим законодательством Российской Федерации общие критерии информационной безопасности. Новизна настоящего исследования заключается в формировании системы специальных критериев безопасности информационных технологий с учетом особенностей применяющего данные технологии субъекта и специфики его деятельности, а именно органа предварительного расследования. В ходе исследования применены методы системного анализа и ситуационного моделирования. Полученные результаты исследования и выводы основаны на понимании сущности правоохранительной деятельности, специфики предварительного расследования, видов субъектов информационного обмена, с которыми взаимодействует орган предварительного расследования в процессе своей деятельности, уровня их информационной защищенности, применяемых информационных технологий, основных видов информации и режимов доступа к ней, практике информационного обеспечения деятельности по расследованию преступлений на примере территориального подразделения органа внутренних дел. По результатам исследования сформулированы критерии безопасности информационных технологий с учетом специфики их вида и особенностей участника информационных отношений. Разработана комплексная модель безопасности информационных технологий органа предварительного расследования, создана система оценки соответствия степени информационной защищенности конкретного участника информационных правоотношений специальным критериям его информационной безопасности.

***Ключевые слова**: кибербезопасность, информационная безопасность, информационные технологии, правоохранительная деятельность, орган предварительного расследования, информационные правоотношения, специальные критерии безопасности, метод ситуационного моделирования, модель информационной безопасности, субъект информационного обмена, информационная система, информационное обеспечение.*

Введение

Критерии информационной безопасности, закрепленные в международных и внутригосударственных правовых актах, являются руководящими принципами по организации системы мер по противодействию угрозам информационной безопасности и разработке правил использования информационных технологий. Указанные критерии условно можно назвать общими критериями информационной безопасности, применяемыми в отношении всех участников информационного обмена.

Основные критерии информационной безопасности также регулируют обеспечение информационной безопасности конкретного участника информационных отношений, однако, необходимо учитывать, что в данном случае речь идет о локальном уровне регулирования и особом виде отношений – информационных правоотношений. Вид субъекта информационных правоотношений, специфика его деятельности и связей с другими субъектами, а также используемые в процессе данной деятельности информационные технологии – индивидуализирующие участника информационного обмена характеристики. Их учет наряду с ситуативными факторами должен осуществляться в рамках специальных критериев – структурного элемента общей системы информационной безопасности.

1 Савченко Оксана Александровна, ВГУЮ РПА Минюста России, Москва, vigiitori@mail.ru

Органы предварительного расследования в своей деятельности имеют дело с информацией, средствами ее обработки – информационными технологиями, и источниками информации. В настоящее время достаточно исследованы вопросы общей теории информационной безопасности, в частности, органов государственной власти Российской Федерации (общий уровень регулирования), безопасности отдельных информационных процессов в правоохранительной деятельности и информационных технологий как технических средств, в том числе, применяемых органами внутренних дел (частный уровень регулирования). Тем не менее, на специальном уровне регулирования необходима разработка концепции безопасности информационных технологий конкретного участника информационных правоотношений – органа предварительного расследования, специфика деятельности которого требует выхода за рамки стандартов.

Новизна данного исследования заключается: 1) в разработке модели безопасности информационных технологий для отдельного участника информационных правоотношений – органа предварительного расследования; 2) в формировании системы диагностики степени защищенности в виде шкалы соответствия специальным критериям безопасности информационных технологий, применяемых данным участником информационных правоотношений.

Материалы и методика исследования

Формирование модели информационной безопасности органа предварительного расследования в настоящем исследовании осуществлено через понятие деятельности по расследованию преступлений. Стоит согласиться с мнением Н.П. Яблокова, что одним из ключевых факторов, оказывающих влияние на предмет методики расследования, являются сведения о сфере, в которой совершается преступление [1, с. 85]. В ходе исследования также применены методы системного анализа и ситуационного моделирования. Системный подход является эффективным методом исследования и имеет целью раскрытие целостности исследуемого объекта со сложной структурой, каким является система безопасности [2, с. 59]. Применение в настоящем исследовании метода ситуационного моделирования актуально в условиях необходимости прогнозирования, предвидения возможного развития чрезвычайных ситуаций, включающих угрозы и вызовы национальной безопасности, и фактора внезапности. В рамках настоящего исследования, при разработке системы соответствия степени защищенности информационных технологий диагностируемого объекта специальным критериям его информационной безопасности, используется алгебраический подход, который, по мнению ряда авторов, является эффективным методом оценки уровня безопасности [3, с. 124]. Степень защищенности информационных технологий, используемых конкретным субъектом информационных отношений, оценивается в соответствии с понятием уровня комплексной безопасности, определяемом как интегральная оценка показателей и критериев, характеризующих состояние защищенности критичных элементов системы [4, с. 7].

Правоохранительная деятельность, одновременно являясь инструментом защиты прав, также требует обеспечения ее безопасности, в частности, информационной. Применяемые отдельным субъектом информационных правоотношений информационные технологии должны соответствовать как требованиям внешней безопасности их использования (внешние критерии), так и внутренней безопасности их архитектуры (внутренние критерии). Основные критерии безопасности информационных технологий предусмотрены международными правовыми актами и сформулированы на основе исследования наиболее известных компьютерных устройств, большая часть операционных систем которых широко и повсеместно применяются. В связи с возможной погрешностью при обобщении результатов исследования свойств наиболее распространенных технологий, целесообразно формирование системы специальных критериев безопасности с учетом конкретного вида участника информационных процессов и используемой компьютерной технологии.

В обеспечении информационной безопасности органа предварительного расследования необходимо учитывать следующие факторы: безопасность информационной системы управления, безопасность персональных данных сотрудников органа предварительного расследования, обеспечиваемая подразделениями кадровой службы; этику и культуру использования информационных технологий сотрудником органа предварительного расследования; наличие сетевых соединений, тип и уровень защиты информационной сети (системы), аппаратный комплекс и программное обеспечение; связи с другими участниками информационного обмена; виды информации и режимы доступа. В соот-

ветствии с данным алгоритмом построена логическая структура настоящего исследования.

Так, по мнению А. А. Нечаева, информационная система управления органом предварительного расследования районного уровня должна прежде всего удовлетворять требованиям начальника органа предварительного расследования, его заместителей [5, с. 475]. Тогда как существует более значимый критерий, который должен предъявляться к информационной системе управления и, в том числе, влиять на состояние ее защищенности. Информационная система управления территориальным органом расследования с учетом его специфики должна корреспондировать всей информационной системе государственных органов. При проведении каких-либо операций с персональными данными первоначально должен осуществляется анализ модели возможных угроз информационной безопасности [6, с. 78]. Недоступность личных данных о сотруднике (номер мобильного телефона, адрес места жительства) также является частью информационной безопасности органа предварительного расследования. Виды субъектов информационного обмена, с которыми взаимодействует такой орган предварительного расследования как Следственный комитет Российской Федерации, перечислены в Приказе Следственного комитета Российской Федерации «Об организации предварительного расследования в Следственном комитете Российской Федерации» от 15.01.2011 № 2 [7]. Правила работы с источниками информации зачастую указываются в ведомственных инструкциях по делопроизводству. Анализ основных нормативных правовых актов, устанавливающих требования к знаниям и навыкам, необходимым для прохождения службы и выполнения служебных обязанностей в органе предварительного расследования, показывает, что в названный перечень не включены этика и культура использования информационных технологий. Сотрудник обязан владеть не только знаниями в области информационных технологий и информационной безопасности, но и основами грамотного, нравственного использования информационных технологий в соответствии с целями правоохранительной деятельности. Для демонстрации эффективности разработанной системы специальных критериев информационной безопасности органа предварительного расследования в качестве объекта диагностики выбраны следственное отделение и отделение дознания одного из территориальных подразделений органов внутренних дел.

Результаты исследования

Для создания модели безопасности информационных технологий, применяемых органом предварительного расследования, предлагается следующий алгоритм действий: 1) общий анализ, включающий: а) определение места и роли информационных технологий в структуре деятельности органа предварительного расследования (обеспечивающая, функционально-деятельностная, технико-криминалистическая, ориентирующая), их предмет, функции, устройство, цели и результаты применения, сферы, процессы и явления, затрагиваемые в связи с данным применением; б) определение содержание понятия безопасности органа предварительного расследования и ее видов; в) установление корреляционных связей между понятиями информационных технологий, безопасности и угроз; г) специальных критериев безопасности информационных технологий на основе произведенного анализа; 2) специальный анализ, учитывающий: а) вид участника информационных процессов; б) вид используемых данным участником информационных технологий, их технические характеристики, уровень и степень защищенности; в) организационные связи с другими участниками информационных процессов, вид используемых ими информационных технологий и степень защиты; г) возможные риски в процессе информационного обмена и коммуникации; 3) создание комплексной модели информационной безопасности органа предварительного следствия по результатам специального анализа; 4) апробация созданной модели и корректировка ее структуры по результатам апробации.

По результатам исследования создана система оценки уровня безопасности информационных технологий одного из участников информационных правоотношений – органа предварительного расследования. Данная система представлена в виде шкалы специальных критериев безопасности информационных технологий. Оценка производится с учетом вышеуказанного алгоритма действий по созданию модели безопасности информационных технологий субъекта правоохранительной деятельности. Для экспериментальной диагностики степени защиты информационных технологий выбрано территориальное подразделение органа государственной власти, в функции которого наряду с управлением определенной системой входит взаимодействие с организациями и гражданами. В связи с чем, степень риска угрозы информационной безопасности ввиду не только внутрисистемного, но внешнего взаимодействия, значительно повышается.

В условия рассматриваемой задачи по диагностике степени защищенности информационных технологий конкретного участника информационных процессов входят: 1) условный объект исследования: отделение дознания и следственное отделение отдела внутренних дел; 2) предмет: информационная безопасность условного объекта; 3) структурные подразделения диагностируемого объекта: административный аппарат в лице начальника органа внутренних дел и его заместителей, орган дознания, орган следствия, оперативно-розыскные службы, учетная группа, дежурная часть; 4) используемые в деятельности органа внутренних дел информационные технологии, их вид, уровень и степень защиты; 5) не относящиеся к служебным информационные технологии, применяемые сотрудниками органа внутренних дел в их деятельности (персональные компьютеры, носители компьютерной информации, мобильные устройства связи); 6) органы, организации и граждане, с которыми взаимодействует орган внутренних дел, и виды связей в процессе данного взаимодействия; 7) виды информации и режим доступа к ней всех вышеперечисленных участников информационных процессов.

Рассмотрим подробнее изложенные условия задачи в соответствии с предложенной моделью безопасности органа предварительного расследования и специальных критериев его информационной безопасности. Орган предварительного расследования как вид участника информационных правоотношений относится к субъектам правоохранительной деятельности. Основной операционной системой, установленной на персональных компьютерах сотрудников органа предварительного расследования, является Windows последних версий. Данная система отличается достаточным уровнем защиты, и в то же время является общераспространенной операционной системой, в соответствии с архитектурой которой создается большинство вредоносных программ. В связи с чем, степень защиты данной операционной системы можно считать удовлетворительной. Тем не менее, уровень защиты операционной системы повышается при ее обновлении, необходимо постоянное, своевременное обновление операционной системы, что составляет большую часть всего комплекса защиты компьютерной информации. Например, в одном из территориальных подразделений органов внутренних дел, в связи с использованием устаревшей версии операционной системы, личных компьютеров и электронных носителей, три из одиннадцати компьютеров, являющихся служебным оборудование, были заражены вредоносной программой Win32.Bundpil типа «worm» («червь»). Данное вредоносное программное обеспечение распространяется через флешнакопители посредством исполнения команды «autorun.inf», то есть, при автоматическом запуске, открывании содержимого электронного накопителя. Основными субъектами информационных правоотношений, с которыми взаимодействует орган предварительного расследования, являются: граждане (потерпевшие, подозреваемые, обвиняемые, свидетели, понятые); органы государственной власти; организации; внутрисистемные подразделения (экспертные службы, управления). Информация, являющаяся предметом информационных правоотношений в сфере правоохранительной деятельности, отличается разнообразием видов: криминалистически значимая, оперативно-розыскная, правовая информация, персональные данные, государственная, банковская тайны, информация для служебного пользования. Доступ к данным видам информации может быть как ограниченным, так и свободным. Таким образом, охарактеризовать данную информацию можно как смешанную. Информация открытого доступа, разглашаемая ненадежными участниками предварительного расследования, имеет либо самый низкий уровень защиты или не имеет ее вообще. Тогда как данные оперативно-розыскной деятельности, информация, составляющая один из видов охраняемых законом тайн, имеет наивысшую степень защиты. Таким образом, общий уровень защищенности информации и ее источников в органе внутренних дел оценивается как средний.

Идеальный уровень безопасности информационных технологий в разработанной системе оценки уровня защищенности информационных технологий органа предварительного расследования принимается равным 100% (табл.1). В левой колонке указаны специальные критерии информационной безопасности участника информационных правоотношений. Анализ в соответствии с условием задачи указанных в колонке «Общая информация» сведений осуществляется по трем уровням: А – высокий уровень, В – средний уровень, С - низкий уровень. Учет баллов производится в соответствии со значениями: уровень А - наличие позитивных факторов - приравнивается к 1; уровень В уменьшает значение на 0,5 единиц; уровень С – наличие отрицательных факторов – приравнивается к 0. Переход на уровень ниже означает уменьшение качества защиты. Для получения результата диагностики необходимо под-

считать количество баллов в столбце «Уровни» и вести данные в таблицу специальных критериев безопасности информационных технологий конкретного участника информационных процессов. Общая оценка степени защиты информационных технологий складывается из оценок по каждому пункту критериев и выставляется в нижней строке таблицы (табл.2).

Высшая оценка, которая может быть получена в соответствии с данным классификатором, равняется 11, что составляет 100% безопасности. Количество критериев в классификаторе может быть увеличено для получения наиболее точного результата. Для осуществления диагностики также может быть приглашен специалист. Результат оценки степени защищенности объекта в соответствии с условиями настоящей задачи составил 45%. Для демонстрации секторов с наибольшей вероятностью угрозы информационной безопасности составлена схема соответствия уровня защиты информационных технологий диагностируемого органа предварительного расследования специальным критериям информационной безопасности для данного субъекта (рис.1). Результаты тестирования также могут быть представлены в виде диаграммы с раскрытием уязвимых секторов, таблицы или в иной форме.

Осуществленная экспериментальная диагностика позволяет сделать выводы, что в исследуемом территориальном подразделении органа

Таблица 1.

Критерии оценки степени защиты информационных технологий органа предварительного расследования

Критерии		**Общая информация ***		**Уровни**		
				A	**B**	**C**
1. Вид участника информационных процессов (государственный орган, негосударственная организация, физическое лицо); основное направление деятельности	Предполагаемый уровень обеспечения безопасности	Государственный орган Правоохранительный орган Орган предварительного расследования Территориальное подразделение	Высокий	✓	-	-
	Действительный уровень обеспечения безопасности		Не учтен человеческий фактор (этика и культура использования информационных технологий	-	✓	-
2. Используемые информационные технологии	Вид, наименование	Операционная система OS Windows		-	✓	-
	Класс	Потребительский		-	-	✓
	Уровень, степень защищенности	Средний (пользовательский уровень)		-	✓	-
3. Средства защиты	Аппаратные	Локальная сеть		✓	-	-
	Программные	Антивирусная программа		-	✓	-
4. Доступ к сети Интернет, наличие сетевых соединений	Уровень доступа (корпоративный, пользовательский)	Пользовательский (подключение к сети Интернет обеспечивается сотрудниками с использованием личных средств доступа)		-	-	✓
5. Круг субъектов взаимодействия и информационного обмена		Широкий (граждане, государственные органы, организации)		-	-	✓
6. Виды информации и режимы доступа	Государственная тайна, банковская тайна, персональные данные, общедоступная информация	Смешанные виды (криминалистически значимая, оперативно-розыскная информация, государственная, банковская тайны, персональные данные и др.)		-	✓	-
	Режим секретности, открытый доступ	Смешанные виды		-	✓	-
Результат диагностики:				45,45%		

**(графа заполняется на основе данных о диагностируемом объекте в соответствии с указанными в левой колонке критериями)*

Таблица 2.

Шкала соответствия степени защиты информационных технологий органа предварительного расследования специальным критериям информационной безопасности

Критерии	Возможная наивысшая оценка	Полученное значение
1. Характеристика объекта диагностики 1.1. Наименование органа 1.2. Вид деятельности	не <	1,5
2. Характеристика используемых информационных технологий 2.1. Вид и класс информационных технологий 2.2. Степень и уровни защиты, наличие обновления	не <	1
3. Характеристика средств информационной защиты (программные, аппаратные)	не <	1,5
4. Характеристика сетевых соединений (наличие доступа к сети Интернет, вид сетевого соединения и степень информационной защищенности)	не <	0
5. Характеристика субъектов информационного обмена (надежность и уровень информационной защиты)	не <	0
6. Характеристика вида информации и режима доступа	не <	1
Оценка:	11	5

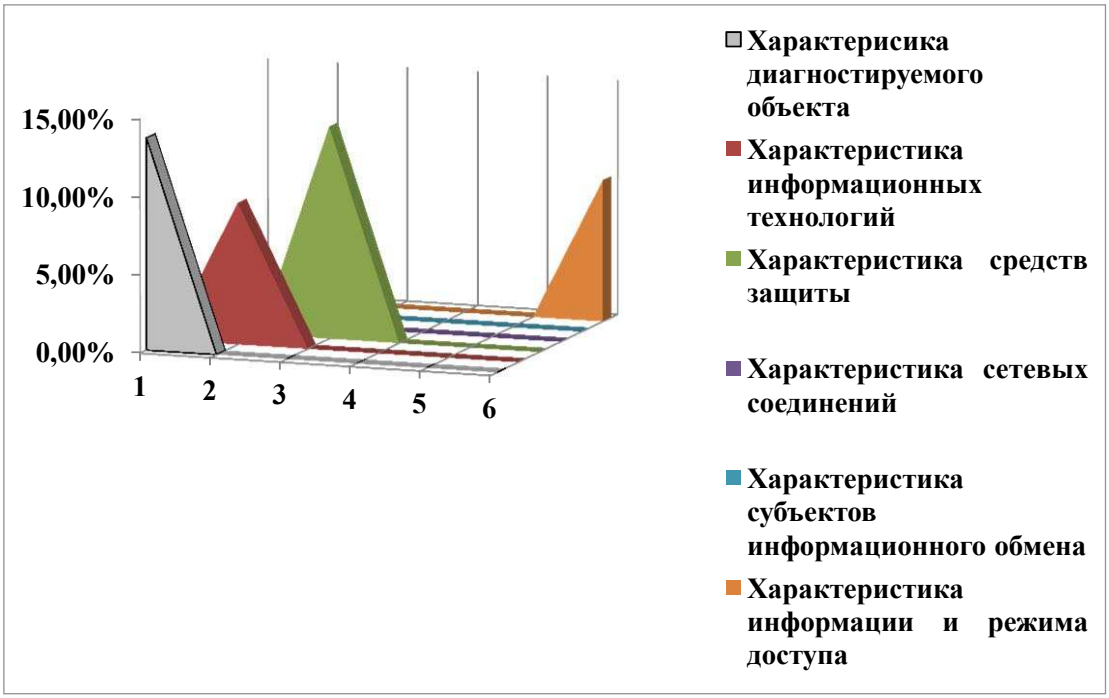

Рис.1. *Соответствие уровня защиты информационных технологий органа предварительного расследования специальным критериям его информационной безопасности*

внутренних дел необходимо: 1) обеспечить сотрудников автоматизированным рабочим местом, локальной компьютерной сетью для внутреннего информационного обмена; 2) обеспечить защиту получаемых данных, применив многоуровневую систему проверки информации; 3) учесть фактор использования персональных технических средств обработки информации сотрудниками в процессе их служебной деятельности.

Специфика служебной деятельности дознавателей, следователей, сотрудников оперативно-розыскной службы заключается в большом проценте работы с информационными источниками. Получаемые в ходе расследования и оперативно-розыскной деятельности сведения, данные, доказательства в форме компьютерной информации зачастую не бывают проверены на наличие угроз. Чаще всего, следователь, дознаватель ввиду боль-

шого объема работы использует как служебную, так и персональную технику. Тогда как вся получаемая компьютерная информация должна быть безопасна для функционирования органа внутренних дел. Носители информации должны проверяться на специально предназначенном для данных целей компьютере с установленной на нем антивирусной программой, и лишь затем информация, содержащаяся на данном носителе, может быть включена в процессы по ее обработке. Правовая культура и правосознание конкретного сотрудника в вопросах этики использования информационных ресурсов имеет немаловажное значение. Недостаточный уровень правовой культуры и правосознания является одним из факторов совершения преступлений в сети Интернет [8, с. 22]. Наиболее высоким уровнем этики безопасного использования информационных источников обладает административный аппарат, службы дежурной части, сотрудники, имеющие допуск к охраняемой законом тайне. Компьютерное оборудование, на котором производится обработка информации для служебного пользования, изолируется от общих сетевых соединений и подключения к нему носителей информации. Необходимо помнить простое правило, что тайна и безопасность данных неразрывно связаны [9, с. 133].

Выводы

Полученные результаты исследования позволяют сделать вывод о том, что специальные критерии безопасности информационных технологий органа предварительного расследования являются необходимым элементом в системе обеспечения информационной безопасности правоохранительных органов. Созданная модель специальных критериев безопасности информационных технологий органа предварительного расследования может применяться наравне с системой информационной безопасности, учитывающей общие критерии и анализ риска [10, с. 104], и рекомендоваться в качестве основы для разработки стратегии информационной безопасности отдельного участника информационных правоотношений – органа предварительного расследования.

Результаты исследования могут быть использованы в области обеспечения деятельности по раскрытию и расследованию преступлений, а также в рамках чтения курса криминалистики, правоохранительных органов в системе высшего образования и курсов повышения квалификации сотрудников органов предварительного расследования.

Выводы основаны на практике прохождения службы в органах предварительного расследования системы внутренних дел, организации обеспечения информационной безопасности международных правоохранительных органов, в частности, на практике применения многоуровневой системы информационной безопасности в подразделениях Интерпола. Классификатор оценки уровня защищенности информационных технологий, применяемых органом предварительного расследования в своей деятельности, разработан по аналогии с оценкой индекса производительности для OS Windows, и может быть дополнен иными критериями в зависимости от вида диагностируемого участника информационных правоотношений и применяемых им информационных технологий.

Научный руководитель: *Колесова Анастасия Сергеевна, кандидат юридических наук, доцент кафедры уголовно-процессуального права и криминалистики Всероссийского государственного университета юстиции (РПА Минюста России), e-mail: nas2481@yandex.ru*

Литература:

1. Яблоков Н.П. Криминалистическая методика расследования: история, современное состояние и проблемы: монография. М.: Норма, 2016. – 191 с.
2. Овчинников В.В., Чумак, С.П., Вдовиченко Е.А., Якутов А.В. Использование системного анализа для определения свойств, связей и метода моделирования технических систем // Технологии гражданской безопасности. 2012. Т. 9. № 3. С. 58-65.
3. Плетнев П.В., Левкин И.В. Алгебраический подход к оценке информационной безопасности // Известия Алтайского государственного университета. 2010. № 1-2. С. 124-127.
4. Ажмухамедов И.М. Анализ и управление комплексной безопасностью на основе когнитивного моделирования // Управление большими системами: сборник трудов. 2010. № 29. С. 5-15.
5. Нечаев А.А. Об информационной системе управления органами предварительного следствия на районном уровне // Организация предварительного расследования. Проблемы и перспективы: материалы Междунар. науч.-практич. конф. (Москва, 20 ноября 2015 г.) / под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. С. 474-478.
6. Еськов А.В., Кирюшин И.И. Защита информационных систем с содержанием персональных данных, эксплуатируемых в ОВД // Проблемы правоохранительной деятельности. 2015. № 2. С. 76-79.

7. Приказ Следственного комитета Российской Федерации от 15.01.2011 г. № 2 «Об организации предварительного расследования в Следственном комитете Российской Федерации». [Электронный ресурс] URL: http//base.consultant.ru.
8. Кананович А.И. Духовно-нравственные факторы совершения преступлений, посягающих на авторские права в глобальной сети Интернет // Российский следователь. 2012. № 21. С. 21-22.
9. Манжуева О.М. Этико-правовые аспекты информационной безопасности // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2014. № 5-2 (43). С. 131-134.
10. Медведев Н.В., Квасов П.М., Цирлов В.Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2010. № 1. С. 103-111.

SPECIAL CRITERIA FOR THE INFORMATION SECURITY OF THE PRELIMINARY INVESTIGATION BODY

Savchenko O.A.[2]

The information security of the preliminary investigation body as a separate participant of information legal relations is an object of this research. The special criteria security of information technology of this separate participant of information processes is a subject of scientific research. The goal of this studies is formulation of information security criteria for special information exchange subject according to his legal enforcement. The relevance of this research lies in necessity of application special criteria to information security of separate participant of information legal relations. The originality lies in creating of system of information security criteria for preliminary investigation body. In this article applied system analysis method, situational modeling method. The results of research based on definition of law enforcement, investigating crimes and on the legal practice of preliminary investigation body. The studies also based on real practice of investigation crimes realized by territorial body of preliminary investigation Ministry of internal affairs. According to the results of scientific research formulated the special security criteria of information technology of legal enforcement body such as preliminary investigation body, specifies the types of this criteria, proposed the integrated security model of information technology, applied by separate participant of information legal relations. Formulated the diagnostic model of information security of preliminary investigation body.

Keywords*: cyber security, information security, information technology, law enforcement, preliminary investigation body, information legal relations, special security criteria, situational modeling method, information security model, information exchange subject, information system, information support*

References:

1. Yablokov N.P. Kriminalisticheskaya metodika rassledovaniya: istoriya, sovremennoe sostoyanie i problemy: monografiya. M.: Norma, 2016. – 191 P.
2. Ovchinnikov V.V., Chumak, S.P., Vdovichenko E.A., Yakutov A.V. Ispol'zovanie sistemnogo analiza dlya opredeleniya svoystv, svyazey i metoda modelirovaniya tekhnicheskikh system, Tekhnologii grazhdanskoy bezopasnosti. 2012. T. 9. No 3, pp. 58-65.
3. Pletnev P.V., Levkin I.V. Algebraicheskiy podkhod k otsenke informatsionnoy bezopasnosti, Izvestiya Altayskogo gosudarstvennogo universiteta. 2010. No 1-2, pp. 124-127.
4. Azhmukhamedov I.M. Analiz i upravlenie kompleksnoy bezopasnost'yu na osnove kognitivnogo modelirovaniya, Upravlenie bol'shimi sistemami: sbornik trudov. 2010. No 29, pp. 5-15.
5. Nechaev A.A. Ob informatsionnoy sisteme upravleniya organami predvaritel'nogo sledstviya na rayonnom urovne, Organizatsiya predvaritel'nogo rassledovaniya. Problemy i perspektivy: materialy Mezhdunar. nauch.-praktich. konf. (Moskva, 20 noyabrya 2015 g.), pod red. A.I. Bastrykina. M.: YuNITI-DANA, 2015, pp. 474-478.
6. Es'kov A.V., Kiryushin I.I. Zashchita informatsionnykh sistem s soderzhaniem personal'nykh dannykh, ekspluatiruemykh v OVD, Problemy pravookhranitel'noy deyatel'nosti. 2015. No 2, pp. 76-79.
7. Prikaz Sledstvennogo komiteta Rossiyskoy Federatsii ot 15.01.2011 g. No 2 «Ob organizatsii predvaritel'nogo rassledovaniya v Sledstvennom komitete Rossiyskoy Federatsii». [Elektronnyy resurs] URL: http//base.consultant.ru.
8. Kananovich A.I. Dukhovno-nravstvennye faktory sovershen'iya prestupleniy, posyagayushchikh na avtorskie prava v global'noy seti Internet, Rossiyskiy sledovatel'. 2012. No 21, pp. 21-22.
9. Manzhueva O.M. Etiko-pravovye aspekty informatsionnoy bezopasnosti, Istoricheskie, filosofskie, politicheskie i yuridicheskie nauki, kul'turologiya i iskusstvovedenie. Voprosy teorii i praktiki. 2014. No 5-2 (43), pp. 131-134.
10. Medvedev N.V., Kvasov P.M., Tsirlov V.L. Standarty i politika informatsionnoy bezopasnosti avtomatizirovannykh system, Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya: Priborostroenie. 2010. No 1, pp. 103-111.

2 Savchenko Oksana, All-Russian State University of Justice, Moscow, vigiitori@mail.ru