СЛЕДСТВЕННЫЙ КОМИТЕТ РЕСПУБЛИКИ БЕЛАРУСЬ

ЦЕНТРАЛЬНЫЙ АППАРАТ СЛЕДСТВЕННОГО КОМИТЕТА
РЕСПУБЛИКИ БЕЛАРУСЬ

ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ И ПЕРЕПОДГОТОВКИ
СЛЕДСТВЕННОГО КОМИТЕТА РЕСПУБЛИКИ БЕЛАРУСЬ

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ

Сборник статей

Минск
«ЮрСпектр»
2020

УДК 343.1 : 004.056 (082)
ББК 67.411я43
П83

П83 **Противодействие** киберпреступности: современное состояние и пути повышения эффективности : сборник статей / Следств. ком. Респ. Беларусь ; редкол.: С. Я. Аземша (гл. ред.) [и др.]. – Минск : ЮрСпектр, 2020. – 322 с.

ISBN 978-985-90478-6-2

Сборник содержит статьи, в которых рассматриваются актуальные вопросы информационной безопасности в условиях развития цифровой экономики, уголовной политики в области обеспечения информационной безопасности, теоретические и практические проблемы расследования киберпреступлений и их профилактики, перспективные направления технико-криминалистической деятельности органов уголовного преследования и подготовки кадров в сфере борьбы с компьютерной преступностью.

Адресуется научным и практическим работникам, преподавателям, аспирантам и студентам учреждений высшего образования.

УДК 343.1 : 004.056 (082)
ББК 67.411я43

ISBN 978-985-90478-6-2

ВАЛОВ Сергей Владимирович,
доцент, кандидат юридических наук,
старший научный сотрудник
научно-исследовательского отдела Московской академии
Следственного комитета Российской Федерации

Организационное обеспечение расследования уголовных дел о киберпреступлениях

Преступности, рассматриваемой в качестве сложного комплексного социального явления, имманентно присуще свойство искать способы и средства, для того чтобы обойти систему контроля, реализуемую в отношении ее общественными и государственными институтами.

Источниками таких способов и средств становятся результаты научно-технического прогресса. Не стали исключением и достижения четвертой промышленной революции, предоставившей человечеству оригинальные сочетания физических, биологических и социальных систем [1, с. 8–14].

Массовое использование различных средств обработки огромных объемов информации, внедрение и доступность портативных средств коммуникации, развитие дистанционных способов доступа к различным материальным и нематериальным благам не могли остаться без внимания преступников и их организаций. На этой технологической основе в указанной сфере произошли существенные качественные изменения – от единичных случаев противоправного использования программно-аппаратных средств до не знающей государственных границ киберпреступности. Во мнениях о характере исходящей от нее угрозы и масштабах наносимого ею вреда сходятся международные организации [2; 3], национальные правительства [4], экспертное сообщество [5, с. 2–18] и специализированные коммерческие организации [6–8].

Вышеназванные изменения оказали непосредственное влияние на рост объемов работы органов предварительного следствия, потребовали принятия соответствующих организационных решений

для адаптации имеющейся в их распоряжении инфраструктуры и кадрового потенциала к расследованию уголовных дел о новых видах преступлений.

Принимая решение о способе организационного обеспечения, субъект управления следственными органами устанавливает организационную связь между спецификой процессуальной деятельности по конкретному уголовному делу или группе уголовных дел и различными характеристиками подчиненного ему сотрудника (профессиональная и должностная компетенция, личные и деловые качества). Соответствующий оперативной обстановке и принципам организационного проектирования способ организационного обеспечения расследования уголовных дел о конкретных видах (категориях, родах) преступлений во многом предопределяет законность, результативность, качество и своевременность защиты прав и свобод личности и публичных интересов от преступных посягательств.

Организационное обеспечение расследования уголовных дел о киберпреступлениях – это осуществляемое на основе облаченного в правовую форму управленческого решения создание новых или преобразование уже существующих временных или постоянных организационно-штатных подразделений следственных органов или определение в них категорий должностных лиц, уполномоченных на постоянной или временной основе производить в соответствии с Уголовно-процессуальным кодексом Российской Федерации предварительное следствие по уголовным делам о запрещенных под угрозой наказания общественно опасных деяниях, совершенных с использованием возможностей, предоставляемых программно-аппаратными комплексами различного назначения, информационными технологиями и коммуникациями, и выполнять иные возложенные на них функции, непосредственно связанные с предварительным следствием.

Результаты анализа нормативных правовых актов и сложившейся практики управления следственными органами в Российской Федерации (вне зависимости от их ведомственной подчиненности) позволяют утверждать, что субъекты управления используют три основных способа организационного обеспечения:

- установление специализации следователей на расследовании отдельных видов киберпреступлений в пределах родовой подследственности;
- создание временных или постоянных организационно-штатных образований (следственных групп или следственно-оперативных групп), предназначенных для объединения усилий должностных

лиц, выполняющих в период производства предварительного следствия взаимосвязанные или взаимодополняющие функции;

- образование в составе следственного органа (от отделения и выше) самостоятельных подразделений (группы, отделения, отделы), объединяющих должностных лиц, выполняющих однородную функцию – расследование уголовных дел о киберпреступлениях.

При выборе способа организационного обеспечения предварительного следствия по уголовным делам о киберпреступлениях субъекты управления учитывают следующие факторы:

- объемы процессуальной деятельности (число находящихся в производстве подчиненных сотрудников уголовных дел в календарный период (месяц, квартал, полугодие, год и более));
- степень сложности расследуемых уголовных дел;
- организационные размеры возглавляемого подразделения (группа, отделение, отдел, управление, департамент, комитет);
- требования вышестоящих субъектов управления к способу обеспечения предварительного следствия по уголовным делам об определенном виде киберпреступлений;
- стратегические и оперативные задачи, стоящие перед подразделением (органом), действующим в определенных условиях оперативной обстановки;
- уровень, занимаемый возглавляемым подразделением (органом) в иерархической системе следственных органов;
- наличие информации о необходимости направления запроса об оказании международной правовой помощи для решения задач предварительного следствия.

Для организационного обеспечения предварительного следствия по уголовным делам о киберпреступлениях, которые крайне редко совершаются на обслуживаемой территории, в следственных органах применяется линейная специализация. Суть данного способа организационного обеспечения состоит в том, что в соответствии с управленческим решением правомочного или уполномоченного субъекта управления на региональном или районном уровне на конкретных должностных лиц (следователей) возлагается обязанность производить на постоянной или временной основе предварительное следствие по уголовным делам о киберпреступлениях.

В тех случаях, когда объем выполняемой работы по уголовному делу требует согласованных действий должностных лиц, правомочных производить предварительное следствие, руководитель следственного органа вправе принять процессуальное управленческое

решение о создании следственной группы (ст. 163 Уголовно-процессуального кодекса Российской Федерации). Если задачи расследования требуют привлечения к их решению потенциала должностных лиц, выполняющих различные правоохранительные функции (предварительное следствие, дознание, оперативно-розыскная или экспертно-криминалистическая деятельность), то по решению руководителя или согласованному решению руководителей различных государственных органов создается следственно-оперативная группа.

В отличие от следственной группы, существующей только в период предварительного следствия, следственно-оперативная группа может быть постоянно действующей. Учитывая особенности совершения киберпреступлений, необходимо задействовать потенциал международных следственно-оперативных групп. От следственной и следственно-оперативных групп следует отличать аналитические группы, состоящие из сотрудников следственных органов. Данные группы также действуют на постоянной основе и призваны изучать уголовные дела, собирать, обобщать и анализировать информацию об однородных преступлениях в целях выявления между ними сходных характеристик по признакам составов.

Увеличение объемов процессуальной деятельности потребовало принятия управленческих решений о создании в составе следственных органов отдельных подразделений, объединяющих сотрудников, специализирующихся исключительно на расследовании уголовных дел о киберпреступлениях. В настоящее время они созданы или на федеральном уровне, или в ряде регионов Российской Федерации, наиболее подверженных киберпреступлениям.

Таким образом, субъекты управления применяют три основных способа организационного обеспечения предварительного следствия по уголовным делам о киберпреступлениях. Выбор способа зависит от ряда объективных и субъективных факторов. Правильность выбора способа предопределяет эффективность и результативность решения задач.

Список использованных источников

1. Шваб, К. Четвертая промышленная революция / К. Шваб. – М. : Эксмо, 2016. – 230 с.
2. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности [Электронный ресурс] : резолюция Генер. Ассамблеи ООН, 22 дек. 2018 г., № 73/266. – Режим доступа: https://undocs.org/ru/A/RES/73/266. – Дата доступа: 06.03.2020.

3. Конвенция о преступности в сфере компьютерной информации ETS № 185 [Электронный ресурс] : [принята в г. Будапеште 23.11.2001 г.] // Консультант-Плюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2020.
4. О Стратегии национальной безопасности Российской Федерации : Указ Президента Рос. Федерации, 31 дек. 2015 г., № 683 // Собр. законодательства Рос. Федерации. – 2016. – № 1. – Ч. II. – Ст. 212.
5. Герке, М. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] / М. Герке. – Режим доступа: www.itu.int/ITUD/cyb/cybersecurity/legislation.html. – Дата доступа: 06.03.2020.
6. Group-IB: топ-10 тенденций из нового отчета High-Tech Crime Trends 2019/2020 [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/group-ib/blog/477958/. – Дата доступа: 06.03.2020.
7. Positive Technologies: Кибербезопасность 2019–2020. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/. – Дата доступа: 06.03.2020.
8. Herjavec Group: 2019 Official Annual Cybercrime Report [Electronic resource]. – Mode of access: https://www.herjavecgroup.com/resources/2019-official-annual-cybercrime-report/. – Date of access: 06.03.2020.

Содержание