УДК 34

Оперативное внедрение как оперативно-тактическая мера, направленная на выявление и раскрытие хищений, совершаемых с использованием вредоносного программного обеспечения

Виноградов Евгений Александрович

Соискатель,
факультет подготовки научно-педагогических
и научных кадров по кафедре оперативно-разыскной
деятельности и специальной техники,
Московский университет МВД России им. В.Я. Кикотя,
117437, Российская Федерация, Москва, ул. Академика Волгина, 12;
e-mail: 40mvd@bk.ru

Аннотация

Оперативное внедрение выступает одним из наиболее сложных, но эффективных мероприятий, позволяющих выявлять и раскрывать не только оконченные хищения, совершенные с использованием вредоносного программного обеспечения, но и подготавливаемые, а также совершаемые преступления. В числе основных этапов оперативного внедрения выделяются получение оснований для проведения оперативного внедрения и его подготовка, составление плана, основой которого выступает разработка легенды и линии поведения внедряемого лица, подведение внедряемого к объекту внедрения, определение места, времени и условий внедрения, а также определение условий вывода из разработки, непосредственное осуществление оперативного внедрения, оформление результатов, полученных в ходе оперативного внедрения. Каждому из указанных этапов присущи свои проблемные аспекты, связанные как со спецификой способов хищений, совершаемых с использованием вредоносных программ, так и со способами их выявления и раскрытия. Четкое законодательное закрепление сущности данного мероприятия, а также установление сущности его основных этапов позволит повысить результативность оперативных подразделений и снизить риск привлечения внедряемых лиц к уголовной ответственности, в том числе по делам о хищениях денежных средств посредством применения вредоносного программного обеспечения.

Для цитирования в научных исследованиях

Виноградов Е.А. Оперативное внедрение как оперативно-тактическая мера, направленная на выявление и раскрытие хищений, совершаемых с использованием вредоносного программного обеспечения // Вопросы российского и международного права. 2025. Том 15. № 7А. С. 98-103.

Ключевые слова

Оперативно-розыскная деятельность; оперативно-розыскные мероприятия; оперативное внедрение; хищения с использованием вредоносного программного обеспечения.

Введение

Преступления, совершаемые с использованием информационно-телекоммуникационных сетей и технологий, в том числе хищения, совершаемые посредством применения вредоносного программного обеспечения, зачастую имеют трансграничный высоко завуалированный характер, когда не только правоохранительным органам не известна информация о членах преступных группировок, их конкретных деяниях и последствиях таковых, но и сами участники преступных сообществ не владеют всеми сведениями о сообщниках, о способах совершения преступления, об уровне негативных последствий, объеме ущерба и т.д. Сказанное предопределяет особую сложность, связанную с выявлением таких противоправных деяний и лиц, их подготавливающих, совершающих или совершивших.

Основная часть

В случае, когда преступление уже совершено, вероятность его выявления и раскрытия повышается при условии, что потерпевший заявляет в правоохранительные органы о факте неправомерного вмешательства в деятельность компьютера, компьютерных систем или иных информационно-телекоммуникационных систем, используемых для оборота денежных средств. Оперативные сотрудники в таких ситуациях используют оперативно-розыскные мероприятия, а именно получение компьютерной информации, прослушивание телефонных переговоров, снятие информации с технических каналов связи, наблюдение и др., которые направлены на сбор и фиксацию информации, свидетельствующую о приискании вредоносного программного обеспечения (например, о покупке программ в даркнете), о состоявшихся договоренностях участников преступления, о распределении их ролей (например, одни участники занимаются поиском и покупкой вредоносных программ и их внедрением в информационно-коммуникационные сети, другие участники подыскивают потенциальных жертв, а также занимаются вопросами перенаправления денежных потоков с банковских счетов потерпевших на счета дроперов), а также о способах совершения преступления (например, использование фишинговых приложений, установка троянских программ и др).

Однако в случае, когда преступление находится в стадии подготовки или в стадии совершения, то есть когда негативные последствия в виде утраты потерпевшими денежных средств еще не наступили, использовать указанные способы выявления вряд ли можно признать достаточно эффективными. Для того, чтобы получать и анализировать информацию, например, передаваемую в телефонных переговорах или посредством использования иных каналов связи (социальных сетей, мессенджеров и др.), изначально необходимо понимать, кто может выступать объектом, представляющим оперативный интерес. Именно при таких условиях наиболее результативным является проведение оперативно-розыскного мероприятия «оперативное внедрение». Суть такого мероприятия, как и названных выше, также состоит в негласном получении оперативно-значимых сведений [Гунич, 2023], но основное отличие, а именно непосредственное участие оперативного сотрудника в деятельности преступной группировки с целью налаживания устойчивого канала поступления оперативно-значимой информации, позволяет в разы увеличить шансы не только на выявление особо опасных хищений, ущерб от которых составляет миллионы рублей, но и на их раскрытие и дальнейшее привлечение виновных к ответственности.

Ни понятие, ни сущность оперативного внедрения не определены на законодательном

уровне, поэтому его содержание раскрывается учеными, которые считают, что оно включает два основных элемента, а именно тактический (проникновение в криминальную среду) и познавательный (сбор разведывательной информации) [Алгазин, Панюшин, 2011]. При этом основными этапами оперативного внедрения выступают:

- получение оснований для проведения оперативного внедрения и его подготовка, в процессе которой оперативные сотрудники осуществляют оценку оперативной обстановки, ведут разработку замысла, устанавливают перечень сил и средств, которые необходимы для реализации мероприятия, а также определяют, какие результаты могут быть получены по итогу проведенного мероприятия. Так, при подготовке оперативного внедрения, осуществляемого в целях выявления хищений, совершаемых посредством использования вредоносных программ, целесообразным видится анализ деятельности лиц, обладающих специальными познаниями в области компьютерных технологий, уровень расходов которых в разы превышает уровень доходов лиц, обладающих схожими компетенциями, а также анализ деятельности юридических лиц, предлагающих определенные услуги в сфере информационно-телекоммуникационных технологий (разработка, продажа и покупка аппаратных и программных комплексов, их обслуживание, управление, аварийное восстановление, услуги по хранению данных на облачных серверах, хостинг и др.);

- составление плана, основой которого выступает разработка легенды и линии поведения внедряемого лица, подведение внедряемого к объекту внедрения, определение места, времени и условий внедрения, а также определение условий вывода из разработки. Основным условием при внедрении в преступную группировку, которая планирует совершать или уже совершает хищения денежных средств посредством использования вредоносных программ, как представляется, выступает наличие у внедряемого специальных знаний в области компьютерных технологий, а также соответствующего материального обеспечения, иначе его расшифровка может стать не только причиной того, что преступник скроется, а дальнейшие действия по его выявлению и поимке будут безрезультативными, но и того, что жизни и здоровью внедренного сотрудника или его родственников будет угрожать опасность;

- непосредственное осуществление оперативного внедрения, которое предполагает сбор информации об участниках киберхищений, способах, которые они используют для совершения преступлений, источниках, из которых поступает вредоносное программное обеспечение (самостоятельная разработка или приобретение на теневых сетевых рынках), средств, применяемых для хищений и дальнейшего перераспределения похищенных денежных средств, а также фиксацию такой информации и ее своевременную реализацию. Однако сбор и фиксация оперативно значимой информации не могут выступать единственной целью оперативного внедрения, поскольку помимо выявления и раскрытия преступлений одной из основных задач оперативно-розыскной деятельности выступает также и их предупреждение. Следует согласиться с теми учеными, которые указывают на такие цели оперативного внедрения, как разобщение участников преступной группировки, дискредитацию лидеров криминальной среды, организаторов и руководителей организованных преступных формирований [Гунич, 2023], достижение которых позволит не просто выявить лиц, планирующих совершение преступлений, но и предотвратить их совершение;

- заключительный этап предполагает вывод внедренного сотрудника, а также оформление результатов, полученных в ходе оперативного внедрения. Определенной актуальностью обладает вопрос, связанный с определением степени участия внедренного в деятельности преступной группировки. Для выявления и раскрытия преступлений, совершаемых в

информационно-телекоммуникационных сетях или посредством их использования, недостаточно просто имитировать преступную деятельность, зачастую оперативникам приходится выполнять конкретные действия, входящие в объективную сторону преступлений, предусмотренных ст. 159.6, 272 или 273 УК РФ. Однако оперативно-розыскным законодательством не урегулирован такой аспект оперативного внедрения, как правомерность привлечения к уголовной ответственности оперативного сотрудника, совершившего преступление в целях недопущения расшифровки и разоблачения.

Заключение

Таким образом, следует сказать, что для выявления и раскрытия как уже совершенных, так и подготавливаемых или совершаемых хищений с использованием вредоносного программного обеспечения оперативные сотрудники используют такое мероприятие как оперативное внедрение. Осуществление данного мероприятия включает несколько этапов, в числе которых следует назвать получение оснований для его проведения, подготовку, планирование, включающее не только разработку легенды и условия введения разрабатываемого в преступную группировку, но и условия его вывода, позволяющие не допустить расшифровку и разоблачение, непосредственную реализацию мероприятия, сбор, фиксацию оперативно значимой информации, а также разобщение преступников и дискредитацию организаторов преступных сообществ, вывод внедренного сотрудника и оформление результатов внедрения.

В числе основных проблем оперативного внедрения, в том числе осуществляемого в рамках выявления и раскрытия киберхищений, следует назвать как несовершенство законодательных норм, а именно отсутствие определения оперативного внедрения, условий уголовной ответственности внедряемого, так и недостаточное организационное и материальное обеспечение его реализации, а также низкий уровень подготовки оперативного состава в сфере информационно-коммуникационных технологий. В этой связи видится необходимым устранение законодательных пробелов, а также повышение уровня знаний и умений оперативных сотрудников.

Библиография

1. Алгазин И.И. Оперативное внедрение: место в структуре оперативно-розыскной деятельности / И.И. Алгазин, Д.Б. Панюшин // Юридические науки и правоохранительная практика. 2011. № 4 (18). С. 71-76.
2. Берова Д.М., Хамгоков М.М. О способах противодействия расследованию преступлений и совершенствовании мер по их преодолению // Государственная служба и кадры. 2019. № 4. С. 167-190.
3. Битов А.А., Токбаев А.А. Понятие и задачи личного сыска в деятельности сотрудника органов внутренних дел // Пробелы в российском законодательстве. Юридический журнал. 2019. № 6. С. 218-221.
4. Борков В.Н. Уголовно-правовая оценка включенности участника оперативно-розыскного мероприятия в преступление // Вестник Санкт-Петербургского университета МВД России. 2019. № 3 (83). С. 97-103.
5. Гунич С.В. Оперативное внедрение: понятие, сущность и содержание // Право и государство: теория и практика. 2023. № 10(226). С. 395-398.
6. Иванов С.И. Особенности взаимодействия при ведении оперативно-розыскной операции органами внутренних дел // Вестник Казанского юридического института МВД России. 2020. Т. 11, № 1. С. 108-112.
7. Ключникова Н.А. Правовая основа деятельности оперативных подразделений // MODERN SCIENCE. 2021. № 11-3. С. 219-224.
8. Михайлов В.И. Правомерный вред — методологическая основа допустимости применения вредоносных мероприятий в оперативно-служебной деятельности правоохранительных органов и специальных служб // Журнал российского права. 2018. № 7. С. 88-100.
9. Толмачева М.А., Ерохин И.В. Сущность оперативного внедрения в оперативно-розыскной деятельности // Приоритетные направления развития науки и образования. Сборник статей X Международной научно-

практической конференции : в 2 ч.. Том Часть 2. 2020. С. 122-124.
10. Шутюк Д.В. Специфика и роль оперативно-розыскной деятельности // Вестник науки. 2023. Том 4. № 12 (69). С. 593-598.

Undercover Operations as an Operational-Tactical Measure Aimed at Detecting and Investigating Thefts Committed Using Malicious Software

Evgenii A. Vinogradov

Applicant for a Scientific Degree,
Faculty of Training Scientific-Pedagogical and Scientific Personnel,
Department of Operational-Search Activities and Special Equipment,
Moscow University of the Ministry of Internal Affairs
of Russia named after V.Ya. Kikot,
117437, 12 Akademika Volgina str., Moscow, Russian Federation;
e-mail: 40mvd@bk.ru

Abstract

Undercover operations represent one of the most complex yet effective measures for detecting and investigating not only completed thefts committed using malicious software but also prepared and ongoing crimes. The main stages of undercover operations include obtaining grounds for conducting the operation and its preparation, developing a plan based on creating a cover story and behavioral line for the undercover agent, introducing the agent to the target, determining the location, time, and conditions of the operation, as well as establishing the conditions for extraction, directly carrying out the undercover operation, and documenting the results obtained during the operation. Each of these stages has its own challenges, related both to the specifics of theft methods involving malicious software and the methods for their detection and investigation. Clear legislative definition of the essence of this measure, as well as the establishment of the essence of its main stages, will enhance the effectiveness of operational units and reduce the risk of undercover agents being subjected to criminal liability, including in cases of monetary theft through the use of malicious software.

For citation

Vinogradov E.A. (2025) Operativnoye vnedreniye kak operativno-takticheskaya mera, napravlennaya na vyyavleniye i raskrytiye khishcheniy, sovershayemykh s ispol'zovaniyem vredonostnogo programmnogo obespecheniya [Undercover Operations as an Operational-Tactical Measure Aimed at Detecting and Investigating Thefts Committed Using Malicious Software]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (7A), pp. 98-103.

Keywords

Operational-search activities; operational-search measures; undercover operations; thefts using malicious software.

References

1. Algazin I.I. Operational implementation: a place in the structure of operational investigative activities / I.I. Algazin, D.B. Panyushin // Legal sciences and law enforcement practice. 2011. No. 4 (18). pp. 71-76.
2. Berova D.M., Khamgokov M.M. On ways to counteract the investigation of crimes and improve measures to overcome them // Civil service and personnel. 2019. No. 4. pp. 167-190.
3. Bitov A.A., Tokbaev A.A. The concept and tasks of personal investigation in the activities of an employee of the internal affairs bodies // Gaps in Russian legislation. Law journal. 2019. No. 6. pp. 218-221.
4. Borkov V.N. Criminal and legal assessment of the involvement of a participant in an operational search event in a crime // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2019. No. 3 (83). pp. 97-103.
5. Gunich S.V. Operational implementation: concept, essence and content // Law and the state: theory and practice. 2023. No. 10(226). pp. 395-398.
6. Ivanov S.I. Features of interaction during the conduct of an operational search operation by internal affairs bodies // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2020. Vol. 11, No. 1. pp. 108-112.
7. Klyuchnikova N.A. The legal basis of the activities of operational units // MODERN SCIENCE. 2021. No. 11-3. pp. 219-224.
8. Mikhailov V.I. Legitimate harm — the methodological basis for the permissibility of the use of harmful measures in the operational activities of law enforcement agencies and special services // Journal of Russian Law. 2018. No. 7. pp. 88-100.
9. Tolmacheva M.A., Erokhin I.V. The essence of operational implementation in operational investigative activities // Priority areas of science and education development. Collection of articles of the X International Scientific and practical Conference: in 2 hours. Volume Part 2. 2020. pp. 122-124.
10. Shutyuk D.V. The specifics and role of operational investigative activities // Bulletin of Science. 2023. Volume 4. No. 12 (69). pp. 593-598.