Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Лукаш Вилим, *Connections QJ* 20, № 2 (2021): 15-20
https://doi.org/10.11610/Connections.rus.20.2.02

Рецензированная статья

Эволюция задач полиции по борьбе с киберпреступностью в Чехии, 2015-2020 гг.

Лукаш Вилим

Министерство внутренних дел Чешской Республики,
https://www.mvcr.cz/mvcren/

Аннотация: В статье рассматриваются расширенные задачи чешской полиции по борьбе с киберпреступностью. Автор подчёркивает важность концептуальных и стратегических факторов появления нового законодательства, финансового обеспечения закупок новой техники и создания новых рабочих мест для специалистов по киберпреступности. Кроме того, крайне важна разработка новых стратегий, соответствующих угрозам, вызовам и возможностям киберпространства. Тесное сотрудничество на всех уровнях системы безопасности может помочь выработке стратегий и тем самым сделать киберпространство более безопасным.

Ключевые слова: киберпреступность, Будапештская конвенция, система безопасности, стратегия, координатор, критическая информационная инфраструктура.

Важным этапом борьбы с киберпреступностью в Чехии стало утверждение правительством 10 июля 2017 г. Концепции развития возможностей чешской полиции по расследованию киберпреступлений (далее – Концепция) под № 502.

Конечно, в этой связи мы не можем не упомянуть о профессионалах, которые занимались киберпреступностью ранее, на местном, региональном и национальном уровне. Определённые изменения в подходах к этому вопросу были внесены ещё в октябре 2015 г., когда Отдел по борьбе с организованной преступностью (*Útvar pro odhalování organizovaného zločinu – ÚOOZ*) начал активно заниматься киберпреступностью. В 2016 г. борьба с киберпреступностью стала частью концептуальной программы созданного

национального подразделения Национального управления по борьбе с организованной преступностью (*Národní centrála proti organizovanému zločinu – NCOZ*). Следует также отметить, что правоохранительные органы обращали внимание на преступную деятельность в киберпространстве с появления Интернета.

Однако вышеупомянутая Концепция впервые в Чехии подошла к проблеме комплексно. Она охватывает разные сферы, существенно усиливая способность чешской полиции бороться с такого рода преступлениями – от наращивания и обучения персонала до законодательных изменений, повлиявших на всю полицию Чехии. В тексте решения об утверждении Концепции, опубликованном также на сайте чешского правительства, сказано, что Концепция

> меняет организацию и штат чешской полиции с 1 сентября 2017 г. Добавляются 30 должностей в чешской полиции, с соответствующим увеличением бюджета для оплаты труда персонала сил безопасности на 4 595 280 чешских крон в 2017 г. Это решение будет иметь долгосрочный эффект в последующие годы, с выполнением требований в 2018 г. и в среднесрочной перспективе на 2019-2020 гг. Выделенный бюджет превысит ранее утвержденные лимиты Министерства внутренних дел … и в 2018 г. появятся 73 новых должности.

Концепция выдвинула высокие требования ко всем, кто участвовал в её реализации и работал над выполнением её условий. Её заслуга в том, что она чётко задала направление выявления, документирования и расследования этого нового вида преступной деятельности. Был усилен персонал, за чем последовала новая система образования, чтобы обучать и готовить сотрудников полиции, занимающихся этой проблемой на всех уровнях.

В законодательстве был изменён Закон № 141/1961 Coll. об уголовном процессе (Уголовно-процессуальный кодекс), касающийся сбора, хранения, использования, обмена и уничтожения данных. Также уделено внимание обнаружению, документированию и расследованию атак на критическую информационную инфраструктуру, включая её защиту от терактов, путем изменений в Законе № 40/2009 Coll., Уголовный кодекс. Конкретно было добавлен новый пункт (e) к первой части Статьи 311 – серьёзные атаки на компьютерные системы, важные для деятельности общества и государства (включая важные информационные системы и критическую информационную инфраструктуру).

Важность Статьи 311 e) заключается в её направленности на теракты в киберпространстве и, соответственно, необходимость защиты конституционной системы и обороны Чехии, а также основных политических, экономических и общественных структур, граждан и международных организаций от политического насилия и экстремизма. Такой теракт может нарушать закон путём ввода данных в компьютерную систему или базу данных либо удаления или повреждения данных, хранящихся в компьютерной системе (базе данных), снижая их качество или приводя их в негодность. Атака на

компьютерную систему может влиять на функционирование государства, здоровье людей, безопасность, экономику или обеспечение базовых потребностей населения. Кроме того, атака с применением специального вредоносного ПО может повредить множество компьютерных систем и нанести большой ущерб.[1]

В 2019 г. упростили ускоренное сохранение данных на компьютерной системе или носителе информации в интересах уголовного процесса, добавив в Уголовно-процессуальный кодекс § 7b, позволивший, при определённых условиях, отдать приказ об ускоренном сохранении данных, важных для уголовного процесса. Согласно § 7b, хранение данных – временная мера, дающая полиции нужное время для защиты данных.[2]

Ещё одна важная норма была введена изменением Закона № 104/ 2013 Coll. «О международном правовом сотрудничестве в уголовных делах». Новый § 65a разрешил ускоренную передачу данных, хранящихся на компьютерной системе на территории другого государства. Этот закон прямо регулирует задачи координатора по вопросам киберпреступности чешской полиции при направлении запросов о предоставлении данных за рубеж с согласия Прокуратуры. У европейских стран хранимые данные запрашивают Европейским следственным ордером. Такой запрос выдаёт или утверждает судебный орган одной страны ЕС, разрешая следственные действия для сбора или использования улик в уголовных делах в другой стране ЕС. Он действует во всём ЕС, кроме Дании и Ирландии.[3] За пределами Евросоюза данные запрашивают на основании договора о взаимной правовой помощи – соглашения между двумя или несколькими странами о сборе и обмене информации во исполнение общего или уголовного законодательства. Запрос в рамках взаимной правовой помощи обычно используют для официального допроса подозреваемого в уголовном преступлении, если подозреваемый живет в другой стране.[4]

Был назначен национальный координатор по вопросам киберпреступности для упорядочения помощи в сотрудничестве и, соответственно, выполнения задач, возникших для Чехии в связи с Конвенцией о киберпреступности Совета Европы (Конвенция о киберпреступности, Будапешт, 23 ноября 2001 г., ETS № 185). Поставленные задачи выполняются круглосуточно и без выходных. Этот координатор также существенно помогает вы-

---

1 Act No. 40/2009 Coll., "The Criminal Code of the Czech Republic," section 311, letter e).

2 Act. No. 141/1961 Coll., "The Criminal Procedure of the Czech Republic."

3 Eurojust, European Union Agency for Criminal Justice Cooperation, "European Investigation Order," доступ на 18 апреля 2021, https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/european-investigation-order-eio.

4 European Commission, "Mutual Legal Assistance and Extradition. Combating Crime Across Borders," https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en.

явлению киберпреступлений и помогает спасению жизней в случае возможных угроз жизни и здоровью в киберпространстве. Чешский национальный координатор по вопросам киберпреступности руководствуется следующими законами и конвенциями:

- Национальный координатор по вопросам киберпреступности согласно Статье 35 Конвенции о киберпреступности (Будапештская конвенция, ETS № 185);
- Координатор согласно Статье 13 Директивы Европейского парламента и Совета ЕС 2013/40/ЕС от 12 августа 2013 г. об атаках на информационные системы – совместно с национальным следственным органом;
- Координатор согласно Протоколу действий правоохранительных органов ЕС в чрезвычайных ситуациях по отражению крупных трансграничных кибератак – совместно с национальным следственным органом;
- Координатор Чешской банковской ассоциации (CBA), администратора домена .cz и национальной группы CSIRT (CZ.NIC);
- Координатор сети G7 24/7 HTC.

Главные задачи, согласно Статье 35 Конвенции о киберпреступности:

- технические консультации;
- хранение данных;
- сбор доказательств;
- предоставление правовой информации;
- установление местоположения подозреваемых и пропавших лиц;
- оперативная связь с другими координаторами.

Четыре года борьбы с киберпреступностью на основе представленной Концепции были успешными. Это подтвердила Резолюция Совета национальной безопасности Чешской Республики от 8 июня 2020 г., одобрившая Итоговый доклад о выполнении задач Концепции развития возможностей чешской полиции по расследованию киберпреступлений. Он же принял решение о разработке новой стратегии борьбы с киберпреступностью.

Судя по дальнейшей динамичной эволюции киберпреступности и по более чем заметному росту преступности в виртуальном мире, для победы над киберпреступностью в будущем понадобится ещё больше усилий. Она потребует внимания со стороны правоохранительных органов и других специалистов в области безопасности, представляющих государство и частный сектор. Киберпространство стало элементом нашей повседневной жизни, который несёт ряд рисков и должен быть надёжно защищён.

В XXI веке придётся заниматься не только общими преступлениями, совершаемыми в виртуальном мире, но и защитой критической информационной инфраструктуры. Это комплексная задача, влияющая на все уровни

системы безопасности и включающая кризисное управление. Нужно понимать, что критическая инфраструктура важна для общества и функционирования демократического государства и является краеугольным камнем процветающей экономики. Поэтому её защита жизненно важна для недопущения перерастания инцидентов в кризисы.

Защиту критической информационной инфраструктуры в киберпространстве можно разделить на три основных уровня: киберзащита, кибербезопасность и киберпреступность. В организационном плане обеспечение безопасности требует эффективных и скоординированных действий вооружённых сил, профильного ведомства кибербезопасности (Национальное управление кибернетической и информационной безопасности; *Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB*), сил безопасности (особенно чешской полиции) и, наконец, разведслужб, а также частного сектора.

Роль государства также заключается в установлении базовых стандартов безопасности и их юридическом распространении на частный сектор. Однако эти меры должны быть финансово обеспечены, и государство обязано обеспечить адекватную защиту киберпространства. Следует помнить, что значительная часть критической инфраструктуры государства не является его исключительной собственностью. Государство лишь участвует в её управлении, в мажоритарной или миноритарной роли.

С этим связана дальнейшая потребность классифицировать киберпреступность, чтобы дать специалистам по компьютерным технологиям возможность выявлять, документировать и расследовать серьёзные киберпреступления, в частности, разного рода атаки на информационную инфраструктуру и важные информационные системы, включая самые серьёзные – терроризм и шпионаж.

Для этого киберпреступность получила новое определение:

- преступление, совершенное в среде информационно-коммуникационных технологий, включая компьютерные сети, где основным объектом нападения является сама область информационно-коммуникационных технологий и содержащиеся в ней данные; отсюда следует, что основное внимание экспертов будет направлено на соответствие установленным критериям – примерами являются § 230 «Несанкционированный доступ к компьютерной системе или носителю информации» и § 231 «Получение и кодирование устройства доступа и пароля к компьютерной системе и другим подобным данным»;
- любое другое преступление, совершённое в киберпространстве, определяемое как преступление, совершённое при значительном использовании информационно-коммуникационных технологий, где главным объектом атаки является жизнь, здоровье, имущество, свобода, человеческое достоинство и мораль.

Заключение

В силу упомянутых выше причин в ближайшем будущем должна быть разработана новая стратегия противодействия киберпреступности, которая должна учесть множество факторов, включая тесное сотрудничество разных партнёров, обеспечивающих безопасность киберпространства. Новая стратегия должна быть представлена Совету безопасности Чешской Республики в 2021 г. Нельзя исключать, что на неё повлияет пандемия COVID-19, вынудившая большую часть общества работать и проводить свободное время в Интернете; для кого-то он стал вторым домом. Наконец, она может касаться киберзащиты от вирусных атак организованных преступных групп и враждебных стран на критическую информационную инфраструктуру, а также их расследование. Другим серьёзным вызовом будущего станет борьба с дезинформацией, что, однако, потребует более тесного взаимодействия всей системы безопасности, и не только в Чехии.

Будапештская конвенция о киберпреступности может служить хорошим примером подхода к другим проблемам безопасности в киберпространстве. Поэтому я могу с уверенностью сказать, что Чехия находится на верном пути в борьбе с киберпреступностью, и верю, что в будущем она усилится.

Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнерство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Статья написана при поддержке Министерства внутренних дел Чешской Республики, проект № VI20192022117, «Выявление радикализации в контексте защиты населения и незащищённых объектов от насилия».

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторе

Лукаш Вилим – подполковник Национального управления по борьбе с организованной преступностью Министерства внутренних дел Чешской Республики, офицер отдела киберпреступности уголовной полиции и службы расследований в Праге. Получил докторскую степень в Полицейской академии в Праге. Д-р Вилим – выпускник программы кибербезопасности и семинара восточноевропейской безопасности Центра им. Джорджа Маршалла. Электронная почта: lukas.vilim@email.cz