обращение к опыту УПК Турции 2004 г.[1], который в ст. 134-1 закрепляет отдельное и самостоятельное следственное действие: досмотр компьютеров, компьютерных программ и изъятие записей. Такой подход, как представляется, позволил бы развить уголовно-процессуальную и криминалистическую науку в новом и специальном направлении, связанном с анализом компьютерных данных и формированием методик доказывания по компьютерным преступлениям.

Итак, для обеспечения эффективной борьбы с преступлениями в сфере информационных технологий необходимо провести масштабную унификацию и систематизацию уголовного закона, выделить отдельную главу, включающую составы преступлений, связанных с информационными технологиями. Кроме того, важно развивать международное сотрудничество, обучение специалистов, усиление ответственности для виновных и активно информировать население о методах защиты информационной безопасности. Только таким образом можно достичь поставленных задач и обеспечить безопасность в информационном пространстве.

Титов Д.В.

Восточно-Сибирский институт МВД России (г. Иркутск)

Шаевич А.А.

Восточно-Сибирский институт МВД России (г. Иркутск)

Интегрированная модель противодействия киберпреступности

В условиях стремительной цифровизации экономики и общественной жизни киберпреступность приобретает все более трансграничный, организованный и технологически изощренный характер. Это ставит перед государствами, организациями и правоохранительными структурами комплексную задачу: обеспечить не только техническую устойчивость информационных систем, но и правовую основу для эффективного взаимодействия в расследовании и пресечении преступлений, совершаемых в виртуальной среде. Актуальность данной проблемы обусловлена фундаментальным противоречием между глобальной природой киберугроз и национальной ограниченностью юрисдикций, что затрудняет сбор, признание и использование цифровых доказательств за пределами одной правовой системы.

Правовые механизмы становятся ключевым элементом обеспечения процессуальной легитимности и международной взаимопомощи. Так, Н.О. Мороз подчеркивает основу подхода ЕС: «В ЕС используется

[1] Уголовно-процессуальный кодекс Турецкой Республики / науч. ред. В.А. Оровер. Владивосток: ДВГУ, 2015. С. 112.

системный подход для координации сотрудничества государств-членов ЕС в борьбе с киберпреступностью, который имеет правовой и институциональный компонент»[1] – это переводит нормы из деклараций в практику. На операционном уровне эту связку поддерживают европейский ордер на арест и ордер на проведение расследования, а также координация через Европол и Евроюст, что ускоряет выдачу и обмен доказательствами при трансграничных расследованиях.

Эффективность правоприменения упирается в международный характер деяний, потому что различия юрисдикций усложняют розыск и сбор цифровых следов. Р.А. Хачидогов фиксирует ключевую проблему: «Международный характер киберпреступлений препятствует поимке преступников вследствие различного законодательства разных стран. Проблемы возникают и при расследовании и сборе доказательств»[2], поэтому устойчивые каналы взаимной помощи и единые правила «цепочки хранения доказательств» становятся критичными. Вместе с тем даже при высокой гармонизации регулирование отстает от технологической динамики. В.А. Шестак и А.И. Адигамов подчеркивают, что «несмотря на высокий уровень унификации уголовного законодательства, нормативно-правовое регулирование борьбы с киберпреступлениями даже в Европейском Союзе отстает от темпов развития кибернетических технологий»[3] – это обосновывает «скользящую» модель: минимальные общие стандарты и регулярные национальные обновления.

Технологическая часть повышает устойчивость через архитектурные решения и дисциплину процессов, чтобы сужать пространство атаки и ограничивать последствия взлома. Принцип нулевого доверия (zero trust) отказывается от «доверенного периметра», поэтому нешаблонное действие упирается в границы сегментации. На практике это выражается в строгих ролевых моделях доступа, проверке состояния устройств и использовании краткосрочных токенов, в результате компрометация одного узла не приводит к каскадному провалу.

Защита учетных данных дает наибольший профилактический эффект, потому что большинство атак начинается именно с них. Многофакторная аутентификация вместе с централизованной сменой паролей и контролем их

[1] Мороз Н.О. Особенности международно-правового сотрудничества в борьбе с киберпреступностью в рамках ЕС // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». 2018. Т. 4. № 4. С. 87-94. DOI: 10.30914/2411-3522-2018-4-4-87-94.

[2] Хачидогов Р.А. Основные методы противодействия киберпреступности в Российской Федерации // Журнал прикладных исследований. 2023. № 6. DOI: 10.47576/2949-1878_2023_6_128.

[3] Шестак В.А., Адигамов А.И. Современные подходы в законодательстве странчленов ЕС к уголовной ответственности за преступления в киберпространстве // Образование и право. 2020. № 8.

использования снижает вероятность несанкционированного доступа, а аппаратные ключи в критичных зонах уменьшают риск фишинговых атак. Помимо этого система временно блокирует подозрительную активность до подтверждения действий пользователя на проверенных устройствах.

Мониторинг объединяет журналы событий конечных точек, сети, приложений и облака в единую картину поведения, поэтому несигнатурные действия мошенников выявляются раньше. Когда требуется реакция может быть использована технология SOAR[1], она закрепляет типовые действия, разграничивает зоны автоматизации и ручного вмешательства и выстраивает коммуникации ролей, в результате среднее время реагирования снижается. Обманная инфраструктура (honeypot – приманочная система) имитирует благоприятную среду для незаконных действий и позволяет изучать тактики противника, если встроена в реальный контекст сети.

Облака и контейнеры требуют строгого управления доступом без универсальных прав и запрета публичности хранилищ по умолчанию, потому что конфигурационные ошибки быстро масштабируются. Подписанные образы, неизменяемые журналы и сетевые политики в оркестраторах уменьшают скрытые каналы, а управление ключами с учетом юрисдикций сохраняет контролируемость законных запросов. Резервные копии ценны только при регулярной проверке восстановляемости.

Организационные меры удерживают технические меры в рабочем режиме, потому что именно они снижают поведенческие ошибки и убирают ошибочные взаимодействия между компонентами. Независимое подтверждение критичных операций через второй канал отсекает социальную инженерию; типовые шаблоны переписки уменьшают вероятность ошибочных согласований; регулярные тренировки закрепляют устойчивые алгоритмы действий под давлением времени. Финансовый мониторинг дополняет общую картину: сначала выстраивается взаимодействие с платежными провайдерами и биржами, далее применяются процедуры противодействия легализации доходов и проверяются санкционные списки и наконец, при необходимости активы замораживаются, в результате уменьшается прибыль злоумышленников и снижается мотивация атак.

Поэтапное внедрение компенсирует ограниченность ресурсов, потому что сначала закрываются зоны максимального риска. Прежде всего платежи, сторонние интеграции и почта получают базовые меры – многофакторную аутентификацию, сегментацию, контроль конфигураций и проверку восстановляемости. Далее добавляются поведенческая аналитика и приманочные системы, а опыт пользователей закрепляется учениями и независимым аудитом. Одновременно консолидация средств вместо разнородного набора инструментов повышает наблюдаемость и снижает стоимость сопровождения.

[1] Система оркестрации, автоматизации и реагирования на инциденты безопасности.

Модель строится на системном подходе и сравнительно-правовом анализе для сопоставления институтов ЕС с механизмами обмена доказательствами, на структурном анализе архитектур защиты для выявления узлов максимального эффекта и на управленческом синтезе регламентов с метриками, чтобы связать нормы, технологии и воспроизводимые действия.

Например, в ситуации подмены платежных реквизитов социальная инженерия нацеливается на срочный перевод. Поскольку регламент требует независимого подтверждения по номеру из CRM и контрольной фразы, операция блокируется, в результате домен-имитатор попадает в блок-листы и цепочка атаки прерывается.

В другом эпизоде утечка облачного ключа обнаруживается автоматическим поиском секретных данных в хранилищах кода. Поэтому запускается немедленная ротация и временное ограничение чувствительных операций, а выдача секретов переводится в инфраструктуру как код с журналированием, в результате риск повторной компрометации снижается и восстановление проходит предсказуемо.

Подводя итоги, можно заключить, что с учетом особенностей современных киберугроз ни одна из мер защиты, будь то передовой инструмент ИИ, строгая норма закона или отработанный регламент, не способна в одиночку обеспечить устойчивость к атакам. Как показано в статье, подлинная эффективность достигается только через синтез трех взаимодополняющих сфер: правовой, технологической и организационной.

Ключевым выводом является то, что устойчивость рождается не из изоляции, а из интеграции. Наконец, эффективность защиты должна измеряться не количеством установленных систем, а содержательными метриками: временем обнаружения и реагирования, долей инцидентов, остановленных до реализации ущерба, частотой успешных восстановлений. Именно такие показатели позволяют переходить от формального соответствия требованиям к реальной киберустойчивости.

Таким образом, в эпоху, когда киберпреступность становится все более изощренной и глобальной, ответ лежит не в поиске «серебряной пули», а в выстраивании целостной, многомерной и динамичной системы защиты, где право, технологии и управление действуют как единый организм. Только такой подход способен обеспечить не просто безопасность, а восстанавливаемость, предсказуемость и доверие в цифровом пространстве.