УДК 004

Жилкайдаров Р.Р.
старший прокурор (информационной безопасности) по развитию информационно-коммуникационных технологий Института стратегического развития и международного сотрудничества Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, советник юстиции

К ВОПРОСУ О ЗАЩИТЕ IT-ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В настоящее время органы прокуратуры активно инициируют использование информационных технологий в правоохранительных органах Казахстана. Не секрет, что отдельные ведомства давно проводили работы по созданию удобной в использовании процессуальной платформы для решения собственных задач. Предполагалось, что данная платформа должна функционировать в едином стандарте правоохранительных органов.

Главный руководитель органов прокуратуры Республики Казахстан, дал указание внедрять программные продукты Е–уголовное дело (далее – «Е-УД»), Е-административное дело (далее – «Е-АД»), а также обучать сотрудников грамотно использовать их и помогать разрешать возникающие технические проблемы [1]. С течением времени пользователи, по разные стороны этих продуктов, смогут оперативно документировать и приобщать собранные доказательства, проводить следственные действия и необходимые в интересах следствия экспертизы, не вступая в физический контакт и не покидая своего рабочего кабинета.

В настоящий момент следователь не сможет изъять процессуальный документ – лишь дополнить дело очередным. Представители защиты получат возможность своевременно изучать материалы и быстрей реагировать на нарушения уголовного производства. Органы прокуратуры, в установленном законодательством порядке, осуществлять надзор. Суды – оперативно рассматривать дела, для которых не нужны огромные судебные залы. Очевидно, что с введением электронного процессуального документооборота у сотрудников государственных органов ответственность за качество работы только возрастет.

Указанный документооборот – это реальность развитых стран мира. Для нас это очевидный плюс – нет необходимости «изобретать велосипед».

По сути, в любом процессуальном деле существуют: потерпевший, свидетели, доказательства. В бумажном деле личность лиц, устанавливается на основании идентифицирующих документов - паспорт, удостоверение личности. Если в виртуальном мире геймеров есть вымышленные образы, то в мире следствия – это неприемлемо. У каждого физического лица есть свой индифицирующий признак его уникальной личности: отпечаток пальца руки, фрагмент ДНК или электронно-цифровая подпись (далее – «ЭЦП»). Использование ДНК-анализа в существующих технологиях довольно затратное занятие по времени и финансам. Использование ЭЦП регламентируется Постановлением Правительства Республики Казахстан от 17 апреля 2004 года N 430 «Об утверждении Правил электронного документооборота». ЭЦП использовалась еще с ввода портала «электронного правительства» для подачи документов в государственные органы.

Например, в суде рассматривают гражданское дело, где несколько свидетелей проживают в разных городах Казахстана. Дабы не затрачивать невосполняемый ресурс - время и сопутствующие к нему финансовые расходы, связанные с проездом, проживанием, питанием, одна из сторон дела ходатайствует о приобщении показаний, которые поступили в районный суд по egov.kz с использованием ЭЦП. Подписанные с применением ЭЦП документы по законодательству дают право представлять интересы в гражданском процессе наравне с письменными [2; ст. 61].

В настоящее время ставится под сомнение использование в юридической практике ЭЦП, так как в суде вызывает сомнение – сам ли гражданин либо процессуальное лицо

использовал электронную подпись? Есть другие варианты использования верификации по биометрическим параметрам [3].

В текущей ситуации правоохранительные органы испытывают очевидные проблемы с техническим обеспечением и специалистами в области информационной безопасности. Рискнем применить к проблеме известный закон Парето в иной интерпретации. На 20% грамотных в IT-технологиях сотрудников правоохранительных органов приходится 80%, которым требуется помощь указанных 20% специалистов. Из вышеуказанных 20% не наберется и пятая часть специалистов, имеющая сертификаты по информационной безопасности. Исходя из изложенного: не следует пренебрегать помощью гражданских специалистов до тех пор, пока в достаточной мере не будут задействованы собственные ресурсы – грамотные в юриспруденции и в IT-технологиях.

Есть мнение, что Е-УД не в достаточной мере защищено. Якобы, технические специалисты, обслуживающие серверное оборудование, легко смогут получить доступ к конфиденциальной информации, содержавшейся в материалах дел.

Подобные утверждения неприемлемы для IT-специалистов. Системы управления баз данных хранят большие массивы цифровой информации на жестких дисках, разбитых на фрагменты. Системотехники, обслуживающие серверное оборудование, на котором хранится охраняемая информация, даже при условии получения доступа к жестким дискам не смогут собрать пазлы мозаики без специального программного обеспечения. Документы после ввода их электронную форму уголовного дела становятся цифровыми кодами, доступными только для чтения. На входе и выходе устанавливаются аппараты шифрования, эффективность которых зависит от алгоритма шифрования и длины ключа. Изменение, редактирование документов в базе данных считается невозможным. Есть вероятность, того что на каком-то этапе использования закрытой информации специалист, условно называемый хакер, сможет получить доступ, после чего либо уничтожить, либо модифицировать защищаемую информацию, что соответственно попадает под диспозиции уголовного кодекса.

На этапе противостояния злоумышленникам стоит служба информационной безопасности. Информационная безопасность – затратное по человеческим и финансовым ресурсам предприятие. Первым это оценил бизнес, особенно банковский центр.

В конце мая текущего года бизнесом и государственными структурами восторженно воспринята новость о разрабатываемой Концепции «Киберщита Казахстана», особенно у продавцов серверного оборудования и специализированного программного обеспечения [4]. Данный проект пока не получил финансирования и поддержки в Министерстве финансов.

Поскольку затронут денежный вопрос, следует отметить, что писать вирус – довольно дорогое удовольствие. Если вирус в самом зародыше будет обнаружен и локализован антивирусной программой, то затраты заказчика-разработчика (хакера) вылетят в трубу. Современные вирусы, так называемого нулевого дня, достигли новых технологических прорывов и быстро «мутируют», изменяясь во времени. Антивирусные программы, работающие по сигнатурам, не способны своевременно выявить подобные угрозы. Это позволяет подобным программам скрытно выстраивать цепочку атаки. Если служба информационной безопасности своевременно локализует угрозу, то не даст намерениям злоумышленников осуществиться. Но только на неопределенное время, так как при наличии устойчивого интереса хакер свою работу не прекратит.

Интернет, в списке угроз служб информационной безопасности, занимает определенно высокий рейтинг. Он позволяет злоумышленникам - хакерам из любой точки мира атаковать ресурсы, имеющие доступ к интернет-сети. Уничтожить компьютерные следы противоправной деятельности им позволяют специальные программы «темного интернета», цепочки виртуальных рабочих мест, которые каждые 4-6 часов перезагружаются, уничтожая при этом доказательства противоправной деятельности.

Именно из этих соображений в государственных органах законодательно прописано разделение внутренней (корпоративной сети) и внешней – с выходом в интернет через единый шлюз доступа к Интернету (далее – ЕШДИ) и указывает о необходимости оснащения рабочих мест и централизованного автоматизированного распространения обновлений программного обеспечения [5]. Несоблюдение «Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденных постановлением Правительства Республики Казахстан от 20

декабря 2016 года № 832, влечет привлечение первого руководителя к административной ответственности [6].

Не во всех государственных органах указанное требование соблюдается. Государственные организации, не имея собственных специалистов, вынуждены полагаться на аутсорсинговые компании, основной целью которых является извлечение прибыли. Возможно, из-за этого встречаются внутренняя и внешняя сети на одних и тех же коммутаторах (физически не разделенные). Или разделенные логически на сетевом оборудовании, но входящие из одной и той же магистрали.

В архитектуре сети организаций встречаются нелепые подключения, когда сетевые коммутаторы последовательно подключаются один к другому, напоминая «елочку». В случае одного плохого контакта такого соединения не работает вся сеть, доставляя определенные неудобства сотрудникам.

Хакеры также используют уязвимости программных продуктов. Эти уязвимости присутствуют и в операционных системах и их периодически публикуют. Для устранения уязвимостей используют заплатки (программы), которые локализуют уязвимости. Важно их установить раньше, нежели уязвимости будут использованы хакерами. Для лицензионных программных продуктов заплатки выпускают сами производители. В программах же, написанных собственными силами, приходится рассчитывать на собственные ресурсы для обеспечения информационной безопасности.

Но, пожалуй, самая реальная угроза исходит от самих сотрудников. Они, не осознавая последствий своих действий, способны нанести непоправимый вред своей организации. Компании, проводящие аудит информационной безопасности, часто используют один и тот же трюк. Перед офисом, разбрасывают определенное количество USB накопителей (флэшек) с вирусом для определенной деструктивной работы. Из числа сотрудников организации обязательно найдется хотя бы один человек, которому будет интересно просмотреть содержимое найденного накопителя. Это вопрос времени. После того как накопитель (флэшка) окажется в порту, соединенному через устройство с локальной сетью организации, вирус начинает действовать. Попасть в сеть злоумышленникам помогут и мобильные телефоны, подключенные в качестве роутера для сети Интернет, не проходящей через ЕШДИ.

Как упоминалось выше, антивирусные программы, особенно государственных органов (сведения по государственным закупкам программного обеспечения легко найти в открытой сети), не могут их маркировать как вирус с немедленным удалением либо перемещением в карантин. Ситуация усугубляется, когда тело вируса состоит из нескольких компонентов, которые раздельно вполне безобидны. Но после того как проходит очередное обновление программного обеспечения они могут активироваться и начать работу. Причем цепочка событий может быть разной и программироваться хакером индивидуально.

В организации, где имеется инфраструктура информационной безопасности, выявление подобной угрозы (по информации Cisco) может занять от нескольких часов до нескольких месяцев [7; с.33]. Служба информационной безопасности может не среагировать и через какой-либо порт ввода-вывода информация может сливаться заказчику вирусной атаки. Исходя из чего, неиспользуемые порты ввода - вывода рабочих станций и мобильных компьютеров служащих, должны быть закрыты [8].

В бизнесе, где подобные угрозы уже давно известны своими локальными ударами, выработана политика информационной безопасности, технические стандарты, процедуры и правила, которые обязательны для всей иерархии сотрудников и руководства [9].

У государственных органов, в этом плане очевидное преимущество. В качестве аутсорсинга нанимаются частные организации, в составе которых имеются сертифицированные специалисты, в том числе и в области информационной безопасности. Важно лишь при проведении процедуры государственных закупок предусмотреть «тонкости обслуживания» в заключаемых договорах.

Информационная безопасность - это не оперативное подразделение. Но правоохранительные органы, в своем составе имеют оперативные подразделения, способные расследовать совместно с подразделениями информационной безопасности уголовные правонарушения в сфере информатизации и связи, в рамках действующего законодательства [10]. Важен их сформированный инструкциями подход к расследованию выявленных прецедентов.

Информационная безопасность реальная угроза дестабилизации государственного управления. И она в списке национальных угроз [11]. Важно уделять должное внимание не только выявлению и локализации инцидентов информационной безопасности, но и развитию компьютерной криминалистики – форензике [12; с.11]. Данное научное направление сильно развито в Российской Федерации.

Подводя резюме, отметим, что внедряемые органами прокуратуры программные продукты: Е-УД и Е-АД в процессе оптимизации по функционалу решаемых задач, должны совершенствоваться и по информационной безопасности: как по длине крипто-ключа так и по способам дистанционной биометрической верификации. В текущий момент правоохранительным органам следует серьезно отнестись к архитектуре раздельных внутренних локальных сетей от внешних в соответствии с требованиями информационной безопасности. Особое внимание следует уделять совместному обучению специалистов и оперативных сотрудников, особенно их взаимодействию в выявлении киберпреступлений, где есть время только на согласованные четко сформулированные действия.

Список использованных источников:

1. Генпрокуратура представила проект «Е-уголовное дело» /http://profit.kz/news/39520/Genprokuratura-predstavila-proekt-E-ugolovnoe-delo/.

2. Гражданский процессуальный кодекс Республики Казахстан от 31 октября 2015 года № 377-V ЗРК и пп.16 п.1 ст.1 главы 1 Закона Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи».

3. Продукты ООО «Центр речевых технологий» /http://www.speechpro.ru/product/.

4. «Создание «Киберщит Казахстана» /https://www.zakon.kz/4861130-sozdanie-kibershhit-kazakhstana.html, Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)».

5. Пп. 17 и пп. 23 п.6 , а также пункт 15, п.16, п.17, п.п. 3 п.18 главы 1 «Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

6. Пп.2 п. ст. 641 Кодекса Республики Казахстан от 5 июля 2014 года №235-V ЗРК: «Об административных правонарушениях».

7. Годовой отчет Cisco по информационной безопасности за 2017 год, - 33с.

8. Пп. 4 п.20 главы 1 «Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.

9. Международный стандарт ИСО/МЭК 27001: «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования».

10. Глава 7 Уголовного кодекса Республики Казахстан, ЗРК от 3 июля 2014 года № 226-V: «Уголовный кодекс Республики Казахстан».

11. Статья 23 главы 4 ЗРК от 6 января 2012 года № 527-IV: «О национальной безопасности Республики Казахстан».

12. Федотов Н.Н. Форензика – компьютерная криминалистика. – Москва: Юридический Мир, 2007.