

Цифровая криминалистика в сфере обеспечения безопасности бизнеса от киберугроз

Научный руководитель – Белавин Андрей Вениаминович

Маслов Николай Васильевич

Аспирант

Московский университет Министерства внутренних дел Российской Федерации,
Факультет заочного обучения, Москва, Россия

E-mail: maslov-narod.group.ru@mail.ru

В современном мире наблюдается рост самых различных киберугроз, что делает сегодня задачу обеспечения информационной безопасности в малом и среднем бизнесе, и в частной жизни граждан актуальной как никогда. В данном сегменте наиболее остро ощущается нехватка квалифицированного IT-персонала, именно здесь бюджет IT-инфраструктуры чаще всего формируется по остаточному принципу, и, наконец, нередко просто отсутствует понимание того, зачем всё это нужно и как всё это делать, и не секрет, что эффективность деятельности IT-специалистов нередко просто некому оценить, поскольку руководство компании, как правило, слабо разбирается в вопросах IT-безопасности, совершенно справедливо полагая, что для этого и должны существовать специально обученные профессионалы.

Вопросы криминалистического обеспечения безопасности бизнеса в свете защиты от киберугроз определяются пониманием самой сути киберугроз, и вопросами эффективного противодействия им. Во-первых, это даёт понимание — защита от каких именно рисков наиболее важна в данной конкретной компании, и, во-вторых, позволит определиться с тем, какие средства для этого потребуются. В каких-то случаях достаточно установки самых обычных антивирусных программ на несколько имеющихся в наличии компьютеров. Таким образом, затраты на IT-безопасность — как финансовые, так и организационные — должны быть пропорциональны тем потерям, которые может понести организация в случае развития ситуации по наихудшему сценарию.

Киберугрозы сегодня подразделяют на внешние, источники и причины которых находятся вне ваших компьютеров и вашей компании, обычно — в глобальной сети, и внутренние, зависящие в первую очередь не от каких-то абстрактных злоумышленников из интернета, а от вашего собственного персонала, оборудования и программного обеспечения.

К внешним киберугрозам относятся, в частности, всевозможные компьютерное вредоносное программное обеспечение, скрытно проникающее в компьютерные системы. Именно компьютерное вредоносное программное обеспечение на сегодня является главной угрозой — с ними сталкиваются более большинство российских компаний, поскольку «подцепить» их в отсутствие эффективной защиты довольно просто, ведь способов проникновения в компьютер достаточно много: открыть вложение в электронном письме, проникновение через незащищённую локальную сеть, использование заражённых «флешек», оптических носителей, мобильных жёстких дисков. И не мало важным представляется вопрос о наносимом ущербе. Компьютерное вредоносное программное обеспечение уничтожает файлы, нарушает работоспособность программ и компьютеров, использует в своих целях каналы связи, используя трафик, рассылают спам. Большое значение имеет такой тип внешних киберугроз как спам, порой доля спама среди всей электронной корреспонденции сегодня может достигать значительных процентов! Спам расходует интернет-

трафик, забивает каналы связи, отвлекает от работы, вынуждая персонал выявлять среди гор рекламы действительно важную корреспонденцию, которую при таком положении дел несложно и потерять (особенно если используются некачественные бесплатные спам-фильтры с большим процентом ложных срабатываний). Всё это в конечном итоге ведёт к финансовым потерям. Кроме того, спам — это ещё один из распространённых каналов внедрения компьютерного вредоносного программного обеспечения. Опасность представляет и удалённый взлом компьютеров, благодаря которому злоумышленник, находящийся, возможно, на другом конце земли, а может — в офисе конкурента, получает возможность читать и редактировать хранящиеся на его ПК и файл-серверах документы, уничтожать их по своему желанию, внедрять в сеть оппонента какие-то свои программы, следящие за вашими действиями или собирающие какую-то иную информацию (вплоть до незаметного для него видео-/аудионаблюдения через штатные веб-камеры и микрофоны ноутбуков). Так же представляют определённую опасность так называемые фишинговые атаки, при которых пользователь компьютера пользуется поддельным веб-сайтом сайта банка, в котором он держит свой депозит, заведомо не зная об этом, и в этом случае злоумышленники, получив все его реквизиты и пароли, могут проводить транзакции от его имени.

Весьма актуальна защита и от такого типа угроз, как хищение мобильных устройств, в памяти которых может в открытом виде храниться важная информация - финансовая документация, персональные данные сотрудников и клиентов, интеллектуальная собственность, электронная переписка, различные идентификационные данные и пароли.

Из внутренних же угроз наибольшую опасность сегодня представляют уязвимости в компьютерном программном обеспечении. В результате, чем больше программ используется компанией, тем выше вероятность того, что через какую-то из них в вашу систему проникнет вредоносное программное обеспечение. Необходимо отметить, что случайная утечка/распространение конфиденциальных данных стоит на втором месте по опасности: электронные каналы утечки информации, телефоны, планшеты, ноутбуки, «флешки» и мобильные жёсткие диски, которые регулярно теряются и похищаются. Вместе с этим, утечка конфиденциальных данных может быть и не совсем случайной, а вовсе даже преднамеренной, с соответствующими мероприятиями по сокрытию самого факта, важные данные можно утратить из-за выхода из строя носителя электронной информации.

Вышеуказанные типы киберугроз являются основными на сегодняшний день. Очевидно, для полноценной защиты информационного пространства организации, систем хранения и обработки данных требуется не просто установка соответствующего программного обеспечения, а целый комплекс программно-технических, административно-организационных и нормативно-правовых мероприятий. При этом необходимо выполнение определённых условий: во-первых, необходимо обеспечить защиту информации, устройств и носителей при помощи технических средств и программного обеспечения; во-вторых, должны быть созданы нормативные документы, регламентирующие порядок работы персонала с информацией; в-третьих, должен быть разработан комплекс мер, препятствующих утечке информации и доступу к ней неуполномоченных на работу с ней лиц. Причём обеспечение защиты от киберугроз в каком-то одном случае упор делается на защите компонентов ИТ-системы, например, на защите веб-сайта, в другом случае - на защите парка рабочих станций, в третьем случае возможно придётся выделить дополнительные средства на создание отказоустойчивого хранилища данных.

В конечном итоге конкретные вариации обеспечения защиты бизнеса от киберугроз зависят от того, какого именно типа киберугрозы наиболее опасны для данной конкретной компании.

Источники и литература

- 1) Маслов Н.В. «Некоторые вопросы криминалистического обеспечения расследования преступлений экономической направленности». В книге: Право и экономика: междисциплинарные подходы в науке и образовании IV Московский юридический форум. XII Международная научно-практическая конференция (Кутафинские чтения): материалы конференции: в 4.ч. 2017. С.227-230.
- 2) Маслов Н.В. «Применение специальных знаний в процессуальной деятельности субъектов юрисдикции». В сборнике: Российский и международный опыт производства судебных экспертиз. Материалы Международной научно-практической конференции. 2017. С. 105-112.
- 3) Маслов Н.В. «Осмотр места происшествия как составляющая криминалистического обеспечения расследования квартирных краж». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 70-79.
- 4) Маслов Н.В. «Особенности повышения эффективности применения криминалистической фотосъёмки специалистом-криминалистом при производстве процессуальных действий». В сборнике: Интерполитех-2016. Материалы XX Международной юбилейной выставки "Интерполитех-2016". Общая редакция: Маричев Н.С. 2016. С. 267-268.
- 5) Маслов Н.В. «Криминалистическая характеристика преступлений, совершенных лицами, имеющими психические отклонения». В сборнике: Экономика и юриспруденция: теория и практика. Сборник публикаций научного журнала "Globus" по материалам XVII международной научно-практической конференции. 2017. С. 24-28.
- 6) Маслов Н.В. «Криминалистическое обеспечение расследования преступлений, совершаемых лицами с психической патологией». ЛОМОНОСОВ-2017. Электронный ресурс. Министерство образования и науки РФ, Московский государственный университет им. М.В.Ломоносова, Координационный совет по делам молодёжи в научной и образовательной сферах при Совете при Президенте Российской Федерации по науке и образованию. 2017.
- 7) Маслов Н.В. «К вопросу обеспечения расследования преступлений, совершённых лицами с психическими отклонениями». В сборнике: Проблемы совершенствования сотрудничества правоохранительных и иных органов государств-участников СНГ в выявлении, раскрытии и расследовании коррупционных правонарушений. Сборник научных трудов Международной научно-практической конференции: научное электронное издание. 2017. С. 186-190.
- 8) Маслов Н.В. «Обстоятельства, подлежащие выявлению по преступлениям совершённых лицами с психическими отклонениями, и некоторые вопросы криминалистического обеспечения выявления, раскрытия и расследования преступлений, совершаемых лицами с психическими отклонениями». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 65-70.
- 9) Маслов Н.В. «Особенности применения криминалистических средств при производстве процессуальных действий, как элемент криминалистического обеспечения расследования преступлений, совершённых лицами с психическими отклонениями». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 60-65.

- 10) Маслов Н.В. «Типологическая характеристика преступников, имеющих психические отклонения, не исключające вменяемости». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXV международной научно-практической конференции. 2017. С. 114-121.
- 11) Маслов Н.В. «Взаимосвязи элементов криминалистической характеристики преступлений, совершённых лицами с психическими отклонениями». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 55-60.
- 12) Маслов Н.В. «Особенности производства первоначальных следственных действий при расследовании преступлений, совершённых лицами с психическими отклонениями». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 50-55.
- 13) Маслов Н.В. «Взаимодействие следователя с работниками органов дознания, криминалистическое обеспечение выдвижения версий и планирования расследования преступлений, совершённых лицами с психическими отклонениями». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXIII международной научно-практической конференции. В 2 частях. 2017. С. 42-50.
- 14) Маслов Н.В. «К вопросу о вменяемости лиц с психическими отклонениями при расследовании преступлений». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXI Международной научно-практической конференции. Научно-информационный издательский центр «Институт стратегических исследований». 2016. С. 180-185.
- 15) Маслов Н.В. «Проблема повышения эффективности применения криминалистической фотосъёмки специалистом-криминалистом при производстве процессуальных действий». В сборнике: Современные проблемы производства судебных экспертиз и исследований. Сборник материалов Международной научно-практической конференции. 2016. С. 98-100.
- 16) Маслов Н.В. «К вопросу обеспечения расследования преступлений, совершённых лицами с психическими отклонениями». В сборнике: Проблемы совершенствования сотрудничества правоохранительных и иных органов государств-участников СНГ в выявлении, раскрытии и расследовании коррупционных правонарушений. Сборник научных трудов Международной научно-практической конференции: научное электронное издание. 2017. С. 186-190.
- 17) Маслов Н.В. «Некоторые вопросы вменяемости лиц с психическими аномалиями». В сборнике: Раскрытие и расследование преступлений: наука, практика, опыт. Сборник научных статей. Одобрено и рекомендовано к изданию решением Редакционно-издательским советом Московского университета МВД России имени В.Я. Кикотя. Москва, 2017. С. 114-119.
- 18) Маслов Н.В. «Изучение личности преступника, имеющего психические отклонения: особенности эмоционального интеллекта, социального функционирования и качества жизни лиц, страдающих психозами, имеющих значение для криминалистического обеспечения расследования и раскрытия преступлений». В сборнике: Современные проблемы гуманитарных и естественных наук: Материалы XXXV международной научно-практической конференции. 2017. С. 121-129.
- 19) Маслов Н.В. «Некоторые вопросы организации раскрытия и расследования преступлений, совершённых лицами с психическими отклонениями». В сборнике: раскры-

тие и расследование преступлений: наука, практика, опыт. сборник научных статей преподавателей и адъюнктов кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя. Москва, 2017. С. 218-222.