УДК 004.056.53

ПЯТЬ ШАГОВ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А. С. Мосолов
кандидат технических наук, доцент
доцент кафедры техносферной безопасности
Российский химико-технологический университет им. Д.И. Менделеева
E-mail: asmosolov@yandex.ru
Ю.В. Прус
доктор физико-математических наук, профессор
профессор кафедры криптологии и специальных алгоритмов
Российский государственный университет нефти и газа (НИУ)
имени И.М. Губкина
E-mail: prus.y@ gubkin.ru
А.Н. Шушпанов
аспирант кафедры техносферной безопасности
Российский химико-технологический университет им. Д.И. Менделеева
E-mail: vremena@me.com

Аннотация. Предлагается концепция формирования системы обеспечения информационной безопасности предприятия. Приведена последовательность проведения необходимых организационных мероприятий, построения процедур, а также осуществления процессов защиты информации в ходе операционной деятельности предприятия.

Ключевые слова: информационная безопасность, ИТ-активы, ИТ-структура.

ENTERPRISE INFORMATION SECURITY: FIVE MAIN STEPS

A.S.Mosolov, Y.V.Prus, A.N. Shushpanov

Annotation: This article proposes the concept of the formation of an enterprise information security system. The content of the paper is devoted to the sequence of the necessary organizational measures, the construction of procedures, as well as the implementation of information protection processes during the operations of the enterprise.

Keywords: information security, IT-assets, IT-structure.

Приведённая в статье концепция была апробирована на примере двух транснациональных компаний – в одной из них схема встраивалась в уже созданный процесс, корректируя опыт ведения активов информационно-технического отдела (ИТО) предшественниками, во втором случае (новая компания) процессы выстраивались с нуля. В обоих случаях схема показала отличные результаты.

В реальной жизни каждый шаг человека – это совокупность мелких мышечных движений. Так же выстроена и эта статья – каждый шаг будет расписан, как совокупность

небольших целей, которых надо достигнуть, чтобы шаг состоялся, и впоследствии происходил точно так же, как человек шагает – не задумываясь, лишь единым усилием воли.

Шаг 1: Инвентаризация ваших активов

Если сделать небольшое отступление в бытовой сектор, можно с уверенностью сказать, что лишь немногие пользователи некоей абстрактной новой техники начинают работу с ней со вдумчивого изучения инструкции, выделяя из неё главные моменты, особенности и нюансы использования [1, с 155]. Понимание ИТ-активов, знание всех путей и методов, которыми компания получает, обрабатывает и хранит важные данные, знание программно-аппаратного комплекса и даже краткие психологические портреты коллег - всё это и есть та самая «инструкция», которую надлежит написать, приступая к работе, создавая состояние защищённости, называемое «информационной безопасностью».

Дело совести каждого - как её писать, писать ли её вообще, или составить в голове. Если «инструкция» будет иметь объективное отражение - в виде файлов, схем, записей, набросков, то впоследствии будет проще как обучать новых сотрудников, так и передавать дела последователям, если понадобится. Идея инвентаризации и документирования одинаково хороша и для маленького магазинчика в один POS-терминал и один компьютер с CRM, так и для «мастодонтов» в мире бизнеса, филиальных и ритейловых сетей. Для «мастодонтов» это особенно важно, но, как показывает практика, они «забывают» об этом шаге едва ли не чаще, чем частные предприниматели.

Итак, как же реализуется этот шаг?

1.1. **Инвентаризация** в общем смысле. На данном этапе необходимо пройти всю структуру - сервера, компьютеры, сетевое оборудование, носимые устройства, съёмные накопители. Всё, что так или иначе будет контактировать с ИТ-структурой по возможности не должно остаться незамеченным. Не останавливайте этот процесс никогда. Генеральный директор принёс личный ноутбук, чтобы в полдень посидеть с ним под кофе на диване в переговорной, пользуясь гостевым wi-fi? Стоит мысленно включить его в схему. Боссу понравилось, и он повторяет этот процесс изо дня в день? Следует включить процедуру в схему письменно.

1.2. **Интервьюирование**. Вне зависимости от того, пришёл ли ответственный за ИТО человек на работу только что, или уже довольно давно работаете, этот шаг очень важен. Во втором случае он превращается в беседы, планёрки, неформальное общение за ланчем, но суть остаётся той же. Говорить нужно со всеми - со своими ИТ-коллегами, с отделом кадров, пусть будет открыт диалог с провайдером, предоставляющим вам услуги. Зачастую на данном этапе посредством ненавязчивого краудсорсинга выясняются такие “узкие места”, какие и на аудите порой найти сложно.

1.3. Понимание **форм представления информации**. Следует знать, откуда в компанию идёт важная информация. Магазины? Колл-центр? Банки? Партнёры? Филиалы? Может быть, подрядчики? После понимания того, откуда информация приходит, следует понять, какими путями и в какой форме. На этом этапе также можно составить для себя представление о программном обеспечении, системах документооборота и тому подобном в компании. Понять, кто с чем работает, какой софт стоит у людей, какого не хватает? На этом этапе можно попутно выяснить, как дела в компании с лицензиями, не дожидаясь аудита поставщика лицензий.

1.4. **Доступ**. Здесь нет избыточной тщательности, здесь она может быть только недостаточной. У кого есть (или может быть) доступ к той или иной информации? Как вообще у вас с разграничением доступа? Кто из сотрудников может просмотреть конфиденциальные данные, и все ли из них имеют на это право? Есть ли уверенность, что никто из посторонних эти данные не просмотрит? Мы помним о нашем боссе – он в пункте 1.1 пьёт кофе в переговорной с ноутбуком? Кстати, у нас гостевой wi-fi за пределами здания не виден? Проверяли ли мы? На данном этапе возникает самое большое количество

вопросов, и не стоит отметать даже самые очевидные из них. Ведь «дьявол кроется в мелочах», как говорится в знаменитой пословице.

1.5. **Хранение данных**. Разные типы данных, как известно, хранят разными способами. У каждого из этих способов есть свои достоинства, и недостатки. Что-то хранят в базах данных, что-то по директориям, что-то в «облаках», но лучше бы научить пользователей адекватному подходу к хранению данных. Менеджеру удобно хранить заметки по новой продукции в почте? Хороший шанс случайно отправить их случайному адресату. Человеческие ошибки - огромный фактор риска в информационной безопасности, их следует минимизировать.

Добившись успеха по этим пяти пунктам – следует резюмировать шаг. Мы получили некоторое знание, массив данных, и его уже можно оформить, например, как технический регламент по работе с информацией для компании.

Шаг 2: Техноминимализм

Вне зависимости от входящих в моду дзен-практик лозунг “меньше – значит, лучше” достаточно применим в корпоративной среде. Зачастую приходится столкнуться с тем, что за годы работы компания накопила огромный массив данных. К сожалению, не все они нужны. Попробуем разобраться, как с этим быть.

2.1. **Уничтожение информации**. Да, вот так просто. Следует помнить, что вся собранная информация на протяжении своего жизненного цикла подвергается ряду преобразований - её сохраняют, архивируют, пересылают, защищают – а когда она не нужна, её утилизируют. Следует лишь чётко обозначить жизненный цикл информации (см. Шаг 1), и понимание своевременности уничтожения ненужного придёт само собой. Плюс останется больше системных ресурсов для нужного.

2.2. **Ведение архива**. Мы говорим как о рабочей информации, так и о периодическом её архивировании, то есть, о бэкапах. Это действительно следует *вести,* а не бросить на произвол судьбы, однажды внедрив. Архивы подлежат наблюдению и проверке. Следует думать как о структуре хранения, так и о дублировании... и вообще о необходимости архивировать. Именно поэтому этот пункт идёт следом за пунктом 2.1, а не перед ним.

2.3. **Проверка настроек по умолчанию**. Для программ, доменных политик, настроек почтового сервера и прочего. Настройки по умолчанию обычно не подразумевают какой-то ротации информации, она просто лежит и копится. Следует персонализировать систему, приятным бонусом часто становится понимание причинно-следственных связей в её работе, а то и повышение квалификации.

2.4. **Соблюдение собственных правил**. На первом шаге мы закончили тем, что создали техрегламент - теперь надлежит ему следовать. Мы получили лаконичный набор правил и методик, который, в принципе, соответствует нашей идее техноминимализма. На то мы и старались сделать их как можно лаконичнее. Так, создавая профиль пользователя для некоего «усреднённого» сотрудника («ещё один бухгалтер!»), нам не надо помнить, что ему надо настроить, какой принтер дать, какие ресурсы в сетевом окружении подключить - всё это есть в правилах. Мы не забываем про автоматизацию – она сделает вышеописанное лучше нас. Но за ней тоже надо следить.

2.5. **Сохранение информации** – зачастую, самый скучный процесс. Законодательство многих стран требует от предпринимателя сохранения информации. Иногда дело бывает не в законодательстве, а в коммерческих причинах. С такой информацией придётся столкнуться. В некоторых компаниях целые комнаты заставлены распечатками такой информации - но к ней никто никогда не обращается. А хранить надо. Здесь точно потребуется ещё один регламент, в котором следует описать, что именно должно быть сохранено, как, где, кого туда впускать, и что делать, когда срок хранения истёк.

Теперь, когда административные вопросы по большому счёту, описаны, время перейти к рабочим моментам. Некоторые аспекты, озвученные выше, будут рассмотрены нами более широко в приложении к непосредственной деятельности.

Шаг 3: Непосредственная деятельность

Даже специально делегированные люди в крупных корпорациях, где их деятельность расписана буквально по пунктам чётких должностных инструкций, смущаются от вопроса: «А чем, собственно, ты занимаешься?» Этот шаг посвящается непосредственно процессам защиты информации в ходе операционной деятельности предприятия [2, с 72].

3.1. **Физическая безопасность**. Идеальный способ «сломать сервер» - это сломать его физически. Информационная безопасность связана с ограничением доступа, и физический уровень ограничения – один из самых важных. Не стоит недооценивать старую-добрую дверь и старый-добрый замок.

3.2. **Шифрование данных**. Во всех его проявлениях, вплоть до стеганографии. Тема, о которой можно говорить довольно долго в рамках отдельной дискуссии. Здесь можно сказать кратко - если есть важные данные, то не надо пренебрегать данной возможностью. Единственное о чём надо помнить – стоимость мероприятий по защите не должна на порядки превышать ценность защищаемой информации. Следует руководствоваться здравым смыслом.

3.3. **Антивирусная защита**. Предсказуемо, но не настолько банально, чтобы не обращать внимания на это важный аспект. Выбор хорошей антивирусной программы в корпоративном оснащении (с удобным управлением, механизмами распространения и мониторинга), регулярное получение обновлений - это очень важно в современном мире, когда вирусные волны могут в одночасье парализовать критически важные направления деятельности, как это бывало не раз.

3.4. **Пароли**. Может показаться, что весь этот шаг состоит из очевидностей, но как показывает практика, всё ещё многим в наши дни это неочевидно. Пароли должны быть комплексными, хорошо бы их периодически менять. Иногда предоставлять пользователям привилегию задавать пароли самостоятельно (без подключения регламентов вида “пароль должен быть не короче n символов, в пароле должны быть прописные и строчные буквы, а также знаки пунктуации”) – это плохая идея. Идея ещё хуже - записывать пароли пользователей в любом виде.

3.5. **Обучение пользователей**. Прочность цепи равна прочности самого слабого звена. Предупреждённый – спасён. Информационную культуру можно привить, воспитать и взрастить, причём не только административно-репрессивно – это крайне немаловажный шаг, который зачастую исключается из поля внимания.

3.6. **Доступ** – мы предлагаем вновь посмотреть на пункт 1.4, но на сей раз в рамках рабочей процедуры. Приведем несколько примеров – скажем, здесь стоит построить рабочий процесс так, чтобы о конфиденциальной информации люди, не авторизованные с ней работать, должны знать максимум то, что она существует, в идеале - чтобы не знали и этого. Ещё обязательно следует разработать процедуру, по которой у человека можно отобрать все способы доступа за минимальное количество шагов, потому что не все увольняются по собственному желанию. Вообще, доступ – это такой пункт, который нужно держать в голове всё время, как уже было сказано – здесь нет избыточной тщательности.

3.7. **Мониторинг**. Обнаружение и анализ не только каких-то гипотетических угроз, а просто отклонений от нормы, которые могут свидетельствовать о многом, в том числе и о сбоях, поломках и просто подозрительной активности. Аудит в серверных операционных системах, различные сервисы и демоны, функционал прошивок в маршрутизаторах, специальные программные продукты – в современном мире есть целый арсенал средств осуществлять это.

3.8. **Своевременное обновление**. Следует уделять некоторое время чтению списков изменений, исправлений критических ошибок, расширения функционала для приходящих обновлений к программным продуктам. Автоматизация приемлема, но лучше ознакомиться с практикой, не пуская эту важную область на самотёк. За отзывами о критических

обновлениях следует следить в несколько раз пристальнее, следует также проверять, насколько корректно они применились.

3.9. **Контроль провайдеров услуг и аутсорсеров**. Нередка ситуация, что какой-то программный продукт в компании поддерживает сторонний аутсорсер. Некоторые компании вообще ИТ-практики в целом отдают на аутсорс, что является, в целом, лишь вопросом доверия аутсорсеру. Предоставляя доступ третьим лицам, нужно убедиться, что права доступа они получают в необходимой и достаточной мере, не более.

3.10 **Документирование процедур**. Технические регламенты, о которых мы говорили ранее, задают направление, но, как правило, технически недостаточно подробное. Описание даже небольших действий превращает задачу в процесс и экономит время при возврате к процедуре, которую требуется исполнять редко.

Весь спектр текущих задач охватить, разумеется, трудно, но соблюдение этих основных сильно приближает ИТО предприятия к полному охвату.

Шаг 4: Утилизация

Отходы производства, информационные отходы – не просто цифровой мусор (а иногда и не только цифровой), но на самом деле лакомый кусочек для некоторых категорий злоумышленников. Нижеследующие моменты необходимо держать в памяти.

4.1. **Удаление информации** – на этот раз в контексте не удаления, как оно есть, а ответственного подхода к нему. Просто стереть или отформатировать носители недостаточно, в корпоративном секторе приветствуются профессиональные системы удаления данных – у них разные алгоритмы функционирования, одним из самых популярных является перезаписывание стёртой информации случайным набором данных.

4.2. **Утилизация оборудования** – логически продолжающее первый пункт действие, при котором используются устройства для физического уничтожения накопителей информации – при помощи электромагнитного импульса или физической деформации.

4.3 **«Низкие технологии»**. Зачастую в компании используется и обращается информация не только в электронном виде – информация может быть, скажем, распечатана. Нельзя оставлять без внимания этот момент – и технических средств для контроля более чем достаточно [3, с 124]. Контроль очереди печати и измельчители бумаги – крайне важные инструменты.

И последнее, но не в последнюю очередь -

Шаг 5: Ответственность за происшествия

Может пройти довольно много времени, прежде чем компании придётся пережить инцидент «взлома», «утечки», пропажи или порчи данных. Отдельным счастливчикам везёт настолько, что с ними этого вообще не происходит. Никогда не следует расслабляться, не бывает 100% защищённых решений. Если не человеческий фактор, то отказ оборудования. В конце-концов, стихийное бедствие, что достаточно редко, но всё же бывает.

В свободное время, когда всё настроено и работает, дайте себе минутку подумать о поведении в кризисной ситуации. Кризис - это развилка, именно поведение в нём определяет, как пойдут дела в компании дальше. Паниковать в этот момент никак нельзя, время дорого. Надо исправляться. А главное, понять - кто (что) виновато в происшествии, и что делать дальше? Результатом этих размышлений должна стать, конечно же, выработка регламента, а регламент должен включить в себя следующие аспекты:

5.1. **Команда**. Персонал ИТО. Следует чётко представлять роль каждого человека, направлять их усилия именно на тот участок фронта работ, где это необходимо. Кризисные работы - это такие же работы, просто в процедурах что-то пошло не так, первым делом надо выяснить, что именно, исправиться, принять ответственность и жить дальше. Надо думать о возможных последствиях. Надо думать, как починить всё, что поломалось.

5.2. **Планы действий**. Следует проработать как можно больший спектр угроз информационной безопасности компании и разработать хотя бы минимальные планы действий. Что-то подскажет жизнь, что-то опыт знакомых, что-то личный опыт, и даже

обострения фантазии не стоит списывать со счетов. Размышлять хорошо холодным, трезвым умом, пока ситуация гипотетическая.

5.3 **Время**. Единственное слово, которое следует упомянуть в этом контексте - слово «быстро». Время в момент инцидента играет против вас. Не надо затягивать пребывание в состоянии мощного стресса. Ни вам, ни компании лишний стресс не нужен.

5.4. **«Дисконнект»**. В большинстве случаев для проведения стрессового аудита помогает отсоединение от внешнего мира - но тут надо взвешивать все «за» и «против», пользы ли будет больше или вреда. То же самое нужно сказать и об остановке функционирования отдельно взятого сервера (если, скажем, объектом инцидента стал он). Удобно, конечно, изучить все файлы журналов, когда в них не ведётся дальнейшая запись, когда энтропия системы не повышается, но надо подумать, не убивается ли постепенно свою компанию вынужденным простоем. Остановленное сердце удобно оперировать, но запустится ли оно обратно?

5.5 **Информирование**. Во всех случаях следует поставить в известность руководителя. Хорошо бы ставить его в известность после завершения инцидента, со всеми отчётами и рекомендациями, но бывает по-разному. Следует твёрдо изложить следующие пункты: инцидент, прогноз на восстановление, этап проводимой работы.

Таковы пять довольно несложных шагов в области информационной безопасности, о которых, скорее всего, и так все знают, но не все думают, и не все достаточно серьёзно к ним подходят. Автор надеется, что они помогут читателю улучшить свой опыт работы ИТО предприятия, а также быть заранее готовым к любому вызову в области информационной безопасности.

ЛИТЕРАТУРА

1. *Пирогов А.С., Кудряшов С.И., Резниченко С.А., Мосолов* А.С. Создание обучающего удостоверяющего Центра на базе Университета // Материалы XI-й Международной конференции «Современные информационные технологии в образовании, науке и промышленности». М.: РГСУ, 2018. С. 155-158.

2. *Шушпанов А. Н., Мухрыгин И. Г.* О современных аспектах информационной безопасности предприятия // Международная научно- практическая конференция молодых ученых по проблемам техносферной безопасности. М.: РХТУ им. Д.И. Менделеева, 2015. С. 71–73.

3. *Мальцев Н.В., Прус Ю.В.* Применение офисной техники для защиты речевой информации инновационного характера в образовательных организациях // Материалы Всероссийской научно-практической конференции «Комплексная безопасность образовательных организаций: теория и практика ». М.: Изд-во Восточная печать, 2017. С. 123–125.