Организационно-психологические аспекты информационной безопасности

En **Organizational and Psychological Aspects of Information Security**

V. V. Bondarev,
PhD (Mil.), Associated Professor
Moscow State Technical University;
Lecturer
Training Center Informzashchita
bondarevvv@mail.ru

Questions of practical psychological interaction and cooperation in the information protection process, establishing methods and maintaining psychological contact, social engineering methods, conflict theory, information security subjects and their interaction, theory and practice of personnel selection and identifying insiders, work of information security officers with users are considered and top managers on information security issues.

Keywords: psychology, information security, insider, the intruder, protection of information, social engineering, organizational and psychological measures to protect information, motivation, psychological monitoring, automated system, administrator, end user, psycho-type

Рассматриваются вопросы практического психологического взаимодействия и сотрудничества в процессе защиты информации, приемы установления и поддержания психологического контакта, приемы социальной инженерии, теория конфликта, субъекты обеспечения информационной безопасности и их взаимодействие, теория и практика подбора кадров и выявления инсайдеров, работы сотрудников службы информационной безопасности с пользователями и топ-менеджментом по вопросам ИБ.

Ключевые слова: психология, информационная безопасность, инсайдер, нарушитель, защита информации, социальная инженерия, организационно-психологические меры защиты информации, мотивация, психологический мониторинг, автоматизированная система, администратор, конечный пользователь, психотип

Валерий Васильевич Бондарев,
кандидат военных наук, доцент
Московского государственного технического университета им. Н. Э. Баумана;
преподаватель
АНО ДПО «Учебный центр «Информзащита»
bondarevvv@mail.ru

Введение

Участвуя много лет в проведении аудитов информационной безопасности (ИБ) и обладая, извините за нескромность, большим опытом практической и преподавательской работы в области защиты информации, автор, тем не менее, зачастую с трудом мог прояснить для себя ответы на, казалось бы, элементарные вопросы.

Почему пользователи записывают пароль на клочке бумаги и хранят его под клавиатурой или в ящике стола? Почему они не соблюдают правила ИБ? Почему иногда очень сложно мотивировать руководство организации для выделения даже скромной суммы на ИБ-мероприятия? Почему с регуляторами/проверяющими/аудиторами порой сложно найти общий язык? Почему пользователи выбирают нестойкие пароли? Почему мы зачастую склонны недооценивать одни риски/угрозы и преувеличивать другие? Почему организация правового режима защиты коммерческой тайны и конфиденциального делопроизводства на местах во многих случаях продвигается со скрипом? Почему в крупных компаниях нужны политики ИБ, тогда как в малых такой нужды нет (хотя стандарты и «лучшие практики» призывают к их написанию и внедрению)? Почему терпимость к риску в России выше, чем в осталь-

ном мире? Почему то, что срабатывает в одной организации, не срабатывает в другой?

Дать ответы на все эти вопросы может новое, еще не до конца сформировавшееся направление в «классической» ИБ, которому даже названия пока нет. Обычно применяют такие термины, как «организационно-психологические аспекты ИБ», «информационно-психологическое направление в безопасности» и пр.

Кроме того, существует множество других направлений, в которых могут помочь опытные профессионалы-психологи:

- понимание мотивации злоумышленников/нарушителей и поиск методов противодействия им;
- прогнозирование действий внутренних нарушителей;
- доведения до всех заинтересованных сторон (особенно руководства) актуальности ИБ;
- повышение осведомленности в вопросах ИБ;
- формирование эффективной ИБ-команды;
- эффективная работа с конечными пользователями, в частности, понимание их действий.

Следует отметить, что проблема информационно-психологических аспектов ИБ лежит в среде междисциплинарного взаимодействия: права, психологии, информационных технологий и «классической» ИБ.

Для того, чтобы психологи и примкнувшие к ним администраторы безопасности сосредоточили усилия на направлении «главного удара», необходимо вспомнить, как и в какой степени сотрудники организации влияют на уровень ИБ. У вооруженного этими знаниями психолога работа в отношении отдельных категорий сотрудников становится понятной практически до деталей.

Зависимость уровня ИБ организации от деятельности различных категорий сотрудников и должностных лиц организации

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) автоматизированной системы (АС) соответствующими множеству значимых угроз методами и средствами.

Обеспечение ИБ – это непрерывный процесс, основное содержание которого составляет управление рисками через управление людьми, ресурсами, средствами защиты и т. п. Люди – обслуживающий персонал и конечные пользователи АС – являются неотъемлемой частью автоматизированной (то есть человеко-машинной) системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

Уровень ИБ организации существенно зависит от деятельности следующих категорий сотрудников и должностных лиц:

- сотрудников структурных подразделений (конечных пользователей АС), решающих свои функциональные задачи с применением средств автоматизации;
- программистов, осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации;
- сотрудников подразделения внедрения и сопровождения ПО, обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ (задач);
- сотрудников подразделения эксплуатации, обеспечивающих нормальную работу и обслуживание технических средств обработки и передачи информации и системного программного обеспечения;
- системных администраторов штатных средств защиты (ОС, СУБД и т. п.);
- сотрудников подразделения защиты информации, оценивающих состояние ИБ, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы по вопросам обеспечения ИБ (аналитиков), внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);
- руководителей организации, определяющих цели и задачи функционирования АС, направления ее развития, принимающих стратегические решения по вопросам безопасности и утверждающих основные документы, регламентирующие порядок безопасной обработки и использования защищаемой информации сотрудниками организации.

Кроме того, на уровень ИБ организации могут оказывать влияние посторонние лица и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или попытки несанкционированного доступа к информации как локально, так и удаленно.

Рассмотрим эти категории сотрудников более подробно.

Влияние на уровень ИБ со стороны руководства организации

Руководство принимает стратегические решения по вопросам ИБ и утверждает основные документы, регламентирующие порядок функционирования и развития АС, обеспечивающий безопасную обработку и использование защищаемой информации.

Руководство определяет критичность процессов, ресурсов и степень их защиты, а также координирует деятельность по управлению и распределению обязанностей по обеспечению ИБ между службами безопасности и автоматизации.

Без понимания руководством важности решения проблемы ИБ и поддержания комплекса мер обеспечения ИБ на должном уровне эффективную систему обеспечения безопасности создать нельзя.

Руководство должно признать комплекс мер по обеспечению безопасности ИТ частью производственного процесса.

Как сказано в стандарте ISO 27002, высшее руководство должно поставить четкую цель и показать свою заинтересованность в вопросах ИБ и их поддержку, способствовать распространению политики безопасности среди сотрудников организации.

В организации должны проводиться регулярные совещания руководства по вопросам корректировки политики ИБ и координации действий персонала.

Влияние на уровень ИБ со стороны службы информационной безопасности

Наиболее значимым звеном, оказывающим влияние на ИБ, являются аналитики и администраторы средств защиты, контроля и управления безопасностью. Аналитики отвечают за анализ состояния ИБ, определение требований к защищенности различных подсистем АС и выбор методов и средств защиты. Администраторы средств защиты, контроля и управления безопасностью отвечают за эффективное применение специализированных средств защиты.

Влияние на уровень ИБ со стороны подразделения автоматизации

Наиболее существенное влияние на ИБ организации в подразделении автоматизации оказывают специалисты подразделений разработки, внедрения и сопровождения ПО, эксплуатации технических средств и общего программного обеспечения, системные администраторы.

Программисты осуществляют разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации. Влияние программистов может быть непреднамеренным (ошибки) и преднамеренным (закладки, люки). Практика показывает, что ошибки кода всегда присутствуют в любой программе.

Подразделение внедрения и сопровождения ПО обеспечивает штатное функционирование прикладных программ (задач).

Подразделение эксплуатации обеспечивает нормальную работу и обслуживание технических (вычислительных средств и средств телекоммуникации) и общего (системного) программного обеспечения.

Администраторы серверов, приложений, БД и т. п. отвечают за эффективное применение штатных средств защиты и разграничения доступа всех используемых ОС и СУБД.

Для обеспечения ИБ необходимо повышение ответственности на основе регламентации процессов разработки, отладки и внедрения ПО (необходимо разделить сотрудников на группы разрабатывающих, тестирующих, внедряющих и сопровождающих ПО и регламентировать их взаимодействие). Кроме того, необходимо обеспечить четкое разделение и регламентацию обязанностей администраторов служб автоматизации и безопасности.

Влияние на уровень ИБ со стороны сотрудников структурных подразделений организации

Сотрудники структурных подразделений (конечные пользователи системы) решают свои функциональные задачи с применением средств автоматизации. Совершение ошибок сотрудниками способствует порождению угроз, которые затем могут быть использованы злоумышленниками для нанесения вреда организации и ее сотрудникам. К числу таких угроз можно отнести:

- создание предпосылок к осуществлению несанкционированного доступа со стороны других лиц (уязвимостей, каналов проникновения) к критичным ресурсам системы;
- разглашение (утечка) конфиденциальной информации (сведений, составляющих коммерческую тайну организации, персональных данных, паролей и др.);
- заражение рабочих станций вирусами, «троянскими» и другими вредоносными программами (внедрение вредоносных и шпионских кодов);
- создание помех для (или остановка) основных производственных процессов.

Способы нанесения ущерба организации (они же возможные цели злоумышленников):

- порча или утрата материального имущества (технических средств);
- искажение или утрата файлов с важной (ценной, чувствительной) информацией;
- потеря конкурентных преимуществ в результате разглашения сведений, составляющих коммерческую тайну;
- дезорганизация или снижение эффективности производственных процессов (нарушение работоспособности подсистем);
- непроизводительные траты ресурсов (материальных, информационных, операционных, рабочего времени и др.);
- судебные иски к организации, к ее руководителям и сотрудникам (со стороны государственных органов, других юридических и физических лиц);
- потеря деловой репутации организации (с последующей потерей клиентов, партнеров и т. п.);
- физический или моральный ущерб персоналу (сотрудникам) организации или третьим лицам.

Неукоснительное выполнение сотрудниками предписанных ограничительных мероприятий существенно повышает уровень ИБ, так как залог обеспечения надлежащего уровня ИБ, если говорить в целом, – жесткая регламентация всей деятельности сотрудников, сочетающаяся с высокой исполнительской дисциплиной. Необходимо учитывать, что регламентация деятельности сотрудников (непосредственно не подчиненных службе безопасности) может привести к конфликтам, поэтому их дополнительные функции должны быть четко определены в соответствующих утвержденных руководством инструкциях.

Регламентация действий пользователей и обслуживающего персонала автоматизированной системы

Пользователи и обслуживающий персонал как неотъемлемая часть АС сами являются источником внутренних угроз ИБ организации и одновременно могут являться частью системы защиты АС. Поэтому одним из основных направлений обеспечения ИБ является регламентация действий всех пользователей и обслуживающего персонала АС, целями которой являются:

- сокращение возможностей лиц из числа пользователей и персонала по совершению нарушений (как неумышленных, так и преднамеренных);

- реализация специальных мер противодействия другим внутренним и внешним для системы угрозам (связанным с отказами и сбоями оборудования, ошибками в программах, стихийными бедствиями и действиями посторонних лиц, не являющихся частью АС).

Регламентация предусматривает введение таких ограничений и внедрение таких приемов работы сотрудников, которые, не создавая помех для исполнения ими своих функциональных обязанностей (технологических функций), минимизируют возможности совершения ими случайных или преднамеренных нарушений (например, наделение каждого сотрудника (пользователя) минимально необходимыми для выполнения своих обязанностей полномочиями по доступу к ресурсам автоматизированной системы).

Кроме того, чтобы пользователи и персонал как часть системы безопасности АС реализовали свои «защитные возможности», регламентации подлежат вопросы исполнения ими дополнительных специальных обязанностей (функций), связанных с усилением режима ИБ. Так, для защиты от действий посторонних лиц и «подкрепления» вводимых ограничений на действия своих сотрудников на компьютерах АС могут применяться средства защиты, работающие на физическом, аппаратном или программном уровне, что также требует регламентации различных аспектов, связанных с работой конечных пользователей и процессами их администрирования сотрудниками подразделений автоматизации и обеспечения безопасности.

С учетом вышеизложенного, можно сделать вывод: к обеспечению ИБ организации (и в определенной степени к управлению ее безопасностью) должны привлекаться практически все сотрудники, участвующие в процессах автоматизированной обработки информации, и все категории обслуживающего АС персонала (кроме посторонних).

Роли и функции различных категорий сотрудников и подразделений организации в обеспечении ИБ существенно различаются (большинство из них должны лишь исполнять установленные в организации регламенты и правила безопасной работы в АС).

Направления деятельности психологов в области ИБ

К таковым можно отнести:

- совершенствование практики подбора кадров, обращая особое внимание на выявление потенциальных инсайдеров;
- противодействие методам социальной инженерии;
- взаимодействие службы/администратора информационной безопасности с конечными пользователями;
- взаимодействие службы/администратора ИБ с руководством организации.

Рассмотрим эти направления более подробно.

Совершенствование практики подбора кадров

Сразу же необходимо отметить, что предлагаемая попытка выявить потенциальную склонность работника к инсайду не является чем-то из ряда вон выходящим. Подобные подходы практикуются и в других «родственных» областях. К примеру, глубоко обоснованная методика психологической диагностики профессиональной пригодности для работы в правоохранительной системе начала применяться более 15 лет назад в Российской Федерации. Одним из основных документов, регламентирующих психологическое тестирование в правовой практике Российской Федерации, является «Руководство по профессиональному психологическому отбору кандидатов на службу в органы прокуратуры Российской Федерации». В этом руководстве выделено пять факторов профессиональной пригодности, включающих соответствующие им комплексы профессионально важных качеств (ПВК):

- требуемый уровень социальной (профессиональной) адаптации;
- достаточная нервно-психическая (эмоциональная) устойчивость;
- высокий уровень интеллектуального развития, познавательная активность;
- коммуникативная компетентность и активность;
- адекватные организаторские способности.

Но подбор кадров/выявление инсайдеров с учетом аспектов нарушений ИБ имеет свои особенности. Основные усилия при этом необходимо сосредоточить на разработке модели нарушителя.

Нарушения и преступления, в том числе и компьютерные, совершаются людьми. Хорошо известно, что бывают «виртуальные преступления», но «виртуальных преступников» не бывает. В этом смысле вопросы безопасности автоматизированных систем по своей сути во многом являются вопросами человеческих отношений и человеческого поведения.

Исследования проблемы обеспечения безопасности компьютерных систем ведутся в направлении раскрытия природы явлений, заключающихся в нарушении целостности и конфиденциальности информации, дезорганизации работы АС. Серьезно изучается статистика нарушений, вызывающие их причины, личности нарушителей, суть применяемых нарушителями приемов и средств, используемые при этом недостатки систем и средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы, которые могут быть полезны при построении моделей потенциальных нарушителей.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Зная причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради

игры или удовольствия, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Следует заметить, что в отсутствие правил (запретов и ограничений) не существует и нарушителей (нет правил – нечего нарушать), поэтому борьба с нарушениями всегда начинается с установления четких правил (ограничений, политики безопасности).

Злоумышленник – это нарушитель, намеренно, со злым умыслом идущий на нарушение.

При построении модели нарушителя обычно формулируются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя и преследуемых им целях;
- о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа обслуживающего персонала и пользователей системы) или внешними (посторонними лицами).

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

- конечные пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- сотрудники службы безопасности;
- руководители различных уровней.

К посторонним лицам, которые могут быть нарушителями, можно отнести:

- технический персонал сторонних организаций, обслуживающий здания и СВТ (уборщики, электрики, сантехники, ремонтники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- клиенты (представители сторонних организаций и отдельные граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций или лица, действующие по их заданию (в том числе иностранных спецслужб);
- лица, случайно или умышлено нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

Можно выделить несколько основных мотивов совершения нарушений:

- безответственность (некомпетентность, халатность);
- самоутверждение;
- вандализм;
- принуждение;
- месть;
- корыстный интерес;
- идейные соображения.

При нарушениях, вызванных безответственностью (халатностью), пользователь производит какие-либо разрушающие действия, не связанные, тем не менее, со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь против системы» либо ради утверждения в собственных глазах или в глазах коллег.

Нарушение безопасности АС может быть связано с принуждением (шантажом, угрозой), местью, идейными соображениями или корыстными интересами пользователя системы. В этом случае он целенаправленно попытается преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой информации и другим ресурсам АС.

Нарушителей можно классифицировать по различным критериям.

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяет только агентурные методы получения сведений;
- применяет пассивные средства (технические средства перехвата без модификации компонентов системы);
- использует только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяет методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АС (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта);
- как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории, но без доступа в здания и сооружения;

- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону хранилищ данных (серверов баз данных, архивов и т. п.);
- с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться также следующие дополнительные ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, то есть объединения (сговора) двух и/или более нарушителей;
- нарушитель скрывает свои несанкционированные действия от других сотрудников.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов нарушителей. Категории нарушителей должны быть охарактеризованы значениями характеристик, приведенных выше. Для каждой из них можно привести оценку количества сотрудников организации, попадающих под данную категорию нарушителей.

Конечно, приведенная здесь модель нарушителя имеет слишком уж описательный характер, да и отталкиваться от профессии/возраста/пола и прочих «социально-демографических» характеристик работника, подозревая его на этом основании в принадлежности к инсайдерам, не стоит, так как это не слишком-то приблизит нас к требуемому результату. Поэтому для систематизации «всех и вся», выявления инсайдеров и отсеивания «подозрительных» соискателей можно и необходимо использовать различные инструменты, например, опросник MBTI, основанный на идеях Карла Густава Юнга. Описывать применение этого опросника мы сейчас не будем, скажем лишь, что он предназначен для выявления определенных людских психотипов, которые могут более прочих оказаться склонными к инсайду. Косвенным подтверждением действенности такого подхода могут служить результаты исследования Эрика Шоу и Харли Стока «Индикаторы поведенческих рисков для выявления инсайдерских краж интеллектуальной собственности», в котором, в частности, описаны ключевые модели поведения, присущие инсайдерам, виновным в краже интеллектуальной собственности.

Другими словами, для каждого психотипа существуют как достаточно полные описания, так и ключевые характеристики. Чем в большей степени человек им соответствует, тем ярче у него выражен тот или иной психотип. Но даже краткий перечень характеристик позволяет делать выводы о том, на что может оказаться способным тот или иной человек.

Социальная инженерия

Как правило, под социальной инженерией понимают совокупность приемов манипуляции человеком или группой людей с целью преодоления систем защиты информации и копирования или модификации информации ограниченного доступа.

Области применения социальной инженерии:

- финансовые махинации в организациях;
- общая дестабилизация работы организации с целью ее дальнейшего разрушения;
- проникновение в сеть организации для дестабилизации работы ее основных узлов с какой-либо целью;
- фишинг и другие способы получения паролей для доступа к информации ограниченного доступа;
- конкурентная разведка.

Конечно, самое эффективное направление применения методов социальной инженерии – добыча информации.

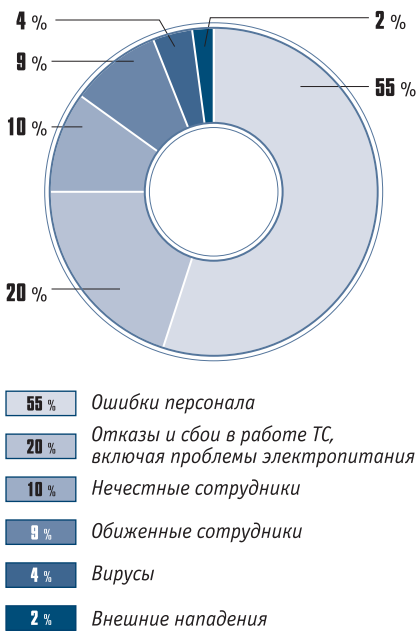
Основным способом защиты от методов социальной инженерии является обучение сотрудников, причем его следует проводить с учетом рекомендаций психологов, учитывающих психотип обучаемого. Все работники компании должны быть документально предупреждены об опасности раскрытия персональной информации и конфиденциальной корпоративной информации, а также о способах предотвращения утечки данных. Кроме того, для каждого сотрудника компании, в зависимости от подразделения и должности, должны существовать инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что обязан сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Взаимодействие администратора безопасности с конечными пользователями

Чаще всего администратору безопасности приходится взаимодействовать с конечными пользователями. Именно они являются основным источником угроз ИБ.

На рисунке приведены результаты анализа нарушений и проблем с ИТ, проведенного Институтом компьютерной безопасности (*Computer Security Institute*).

Как видно из диаграммы, более половины (55 %) проблем возникает из-за ошибок пользователей и об-



Рисунок

служивающего персонала системы. К этому надо добавить нарушения со стороны обиженных (9 %) и нечестных (10 % нарушений) сотрудников организаций.

Согласно одному из последних обзоров аналитического подразделения журнала The Economist, информационная безопасность является одной из приоритетных проблем для 78 % из 254 опрошенных по всему миру первых лиц компаний. Респонденты признавали, что большую часть проблем создают сами сотрудники корпораций. По статистике опроса, источник 83 % проблем с безопасностью находился внутри компании.

Сотрудники организации являются самой массовой категорией нарушителей в силу их многочисленности, наличия у них санкционированного доступа на территорию, в помещения и к ресурсам системы, разнообразия мотивов совершения разного рода небезопасных действий. Причем подавляющее большинство нарушений со стороны сотрудников носит неумышленный характер. Однако ущерб, который они при этом наносят организации, весьма значителен. Именно поэтому борьба с ошибками пользователей и обслуживающего персонала АС является одним из основных направлений работ по обеспечению безопасности.

Возможны два типа подходов администратора к пользователям, склонным к нарушениям правил: доверительный и параноидальный. Последний подход обычно влечет за собой больший урон системе, чем предотвращает. Позиция автора этих строк выражается в его любимом изречении: «Не следует приписывать злонамеренности тому, что можно списать на тупость». Иными словами, большинство пользователей не имеет возможности или знаний для того, чтобы причинить реальный вред системе. В 90 % случаев, когда пользователь является источником проблем для работы системы (например, когда он заполняет пользовательский раздел большими файлами или запускает несколько копий большой программы), он не осознает возможных последствий своих действий. Известны случаи, когда пользователи создавали большие проблемы просто по небрежности.

Администратору при взаимодействии с создающим опасные ситуации пользователем не следует изначально занимать обвинительную позицию. Вместо того, чтобы вступать с конфронтацию, лучше обсудить с ним возникшую проблему. Мало того, что бремя доказательства в любом случае лежит на администраторе ИБ, меньше всего любой из них заинтересован в ссорах с пользователями, поскольку это может вызвать подозрения в том, что администратор некорректно выполняет свои функции. Более того, если пользователь полагает, что администратор не доверяет ему или плохо к нему относится, он может, например, выдвинуть встречные обвинения в чтении или уничтожении чужих файлов.

Допустим, администратор обнаруживает, что некий пользователь пытается осуществить действия, нарушающие корпоративную политику безопасности или способные причинить ей какой-либо вред. В этом случае, если нарушение не слишком серьезное, целесообразнее вынести нарушителю предупреждение о недопустимости совершения подобных действий в дальнейшем.

Даже если подобные действия повторятся, бывает затруднительно доказать, что в действиях нарушителя присутствует злой умысел, а не случайность или небрежность. Тем не менее, во многих случаях пользователя можно «застать на месте преступления», и такие ситуации следует документировать и использовать себе на пользу.

Взаимодействие администратора безопасности с руководством организации

Следует отметить, что руководителями различного ранга не всегда адекватно оценивается значимость мер по информационной безопасности организации. Чаще всего это выражается в игнорировании затрат на обеспечение ИБ ввиду отсутствия представления о риске утраты, нарушения целостности информации, конфиденциальности и доступности обладаемой информации. Администратору безопасности, очевидно, в этой ситуации необходимо инициировать оценку информационных рисков. Попросту говоря, администратор (аналитик, риск-менеджер и т. д.) должен убедить руководство, что если не совершить определенных телодвижений, условно говоря, стоимостью 100 у. е., то организация понесет убытки в 100-кратном размере. Кстати говоря, в мировой практике затраты на защиту информации составляют примерно 10 % от возможных убытков из-за ее утраты, утечки или реализации иных информационных угроз.

Иногда для более удобной работы конечных пользователей руководство «закрывает глаза» на невыполнение ими мер по защите информации. Здесь администратору безопасности важно правильно оценить баланс между удобством использования СВТ и АС и мерами по защите информации, доложив руководству организации свое видение ситуации.

Чтобы добиться от руководства понимания и осознания важности проблем ИБ, необходимо оказывать на него постоянное воздействие, показывая актуальность данной проблемы – учить (информировать) на чужих и собственных примерах (инцидентах). В этих целях можно использовать различные меры и способы, такие как:

- извлечение максимальной образовательной пользы из любых случившихся инцидентов с акцентом на важность решений вопросов по обеспечению ИБ;
- организация собственных показательных мероприятий, например, демонстрации слабости парольной защиты (проведение подобных мероприятий требует предварительного согласования с руководством, документального оформления и осторожности при реализации);
- демонстрация реальных документов других организаций по вопросам обеспечения ИБ.

Выбор конкретных форм и методов работы с руководителем, зависит от характера и темперамента последнего, так как характер и темперамент определяют его стиль, метод,

тип руководства. Данный вопрос детально рассмотрен в работах американских психологов Р. Блэйка и Д. Моутон, в которых для определения типа менеджера разработана матрица типов руководителей. Подробности их исследований широко освещены в литературе и доступны для практического применения.

Кто же будет заниматься всем этим?

В службу компьютерной безопасности могут входить сотрудники с разными функциональными обязанностями:

- руководитель;
- аналитики;
- администраторы средств защиты, контроля и управления;
- администраторы криптографических средств защиты;
- специалисты по защите информации от утечки по техническим каналам;
- ответственные за организацию конфиденциального (секретного) делопроизводства и др.

В идеальном варианте к их числу следует добавить психолога, который решает перечисленные выше задачи. В большинстве организаций его нет и в ближайшей перспективе не будет. Каков выход? «Черновую» работу по проведению тестирования можно поручить, например, HR-отделу. ИБ-служба, в свою очередь, будет работать с уже готовыми характеристиками и выявленными психотипами.

Вкратце алгоритм работы может быть примерно таким. HR-служба «прогоняет» сотрудника по определенному набору тестов. Информация передается в службу ИБ. Зная, к какому типу принадлежит сотрудник, специалист службы определяет его потенциальную склонность к инсайду (должны учитываться не только ключевые характеристики психотипа, но и другие переменные: выраженность предпочтений, склонность к риску, уровень социального интеллекта). Конечно, это примерный алгоритм. Как его реализовать, зависит от масштаба организации, предметной области, в которой она функционирует, критичности ресурсов и еще множества факторов.

И последнее. Как использовать полученные результаты, например, результаты тестирования сотрудника? Здесь все достаточно просто. Если ваш работник – обладатель ярко выраженного психологического (соционического) типа, входящего в «группу риска», то за ним лучше всего «приглядывать». Другой пример – администратор безопасности с учетом типа руководителя организует общение с ним по вопросам обеспечения ИБ.

Что же касается достоверности результатов, здесь тоже не должно возникнуть сложностей. Описанный подход вряд ли способен полностью заменить профессиональный опыт руководителя, оценки экспертов, результаты применения других методов исследования личности. Но зато такие тесты могут компенсировать недостаток профессионального опыта у вышеназванных лиц, оказать помощь в отсутствие экспертов и при невозможности применить другие методы.

Выводы

Основной целью деятельности психологов совместно с HR-службой, сотрудниками службы ИБ, юристами, «автоматизаторами» и пр. является создание гармоничной среды, способствующей развитию сотрудников и всей организации в целом, что предполагает:

- улучшение психологического климата организации и повышение «боевого духа» ее сотрудников, в том числе фокусирование их усилий на защите информации;
- совершенствование практики подбора кадров, особенно при выявлении потенциальных инсайдеров;
- оказание поддержки сотрудникам в развитии их способностей, в том числе направленных на запоминание паролей;
- сплочение коллектива в единую команду, стремящуюся парировать/нейтрализовать угрозы безопасности в отношении организации;
- устранение конфликтов, в первую очередь, между пользователями и сотрудниками ИБ, между сотрудниками ИБ и сотрудниками ИТ;
- снижение текучести кадров, связанной с нарушениями режима ИБ;
- создание атмосферы доверия между сотрудниками ИБ и пользователями, в том числе в деле поддержания режима ИБ;
- проведение разумной политики поощрения и наказания в организации, в том числе создания баланса между административным принуждением и сознательным выполнением регламентов ИБ;
- консультирование руководителей по психологическим аспектам деятельности организации в области ИБ;
- обучение руководителей и сотрудников психологическим технологиям взаимодействия и методам психологической защиты. ■

ЛИТЕРАТУРА

1. *Бондарев В. В. Функционально-системный подход в подготовке специалиста в области информационной безопасности // Сборник трудов конференции. НУК ИУ МГТУ им. Н. Э. Баумана. – М.: 2017.*
2. *Управленческая решетка Блейка-Моутона / Экономический портал [Электронный ресурс]. – Режим доступа: http://www.economicportal.ru/ponyatiya-all/management_lattice.html.*
3. *Бондарев В. В. Учебное пособие. Введение в информационную безопасность автоматизированных систем. – М.: Изд-во МГТУ им. Н. Э. Баумана. – 2016. – 236 с.*
4. *ГОСТ Р ИСО/МЭК 27002 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 года № 423-ст). Дата введения: 01.01.2014.*
5. *«О профессиональном психологическом отборе кандидатов на службу в органы прокуратуры Российской Федерации и обучение в государственные образовательные организации». Приказ Генеральной прокуратуры РФ от 15 сентября 2014 года № 493.*
6. *Психология на службе информационной безопасности. Склонность к преступлению [Электронный ресурс]. – Режим доступа: https://habr.com/post/317066/.*
7. *4BRAIN [Электронный ресурс]. – Режим доступа: https://4brain.ru/blog/.*
8. *Исследование Symantec: психологический аспект краж интеллектуальной собственности в корпоративной среде.*