Известия Гомельского государственного университета
имени Ф. Скорины, № 2 (113), 2019

УДК 159.9:331.101.1

Инженерно-психологические и педагогические методы и средства обеспечения информационной безопасности организации закрытой структуры

К.Р. Ерминек

Исследуется необходимость понимания категории безопасности в качестве понятия, используемого в различных сферах знаний – понятия интердисциплинарного. Целью является характеристика безопасности в аспекте информационном, психологическом и педагогическом. Указываются также взаимосвязи, существующие между указанными аспектами. Содержится также анализ безопасности закрытой структуры, учитывающий психологические индивидуальные и групповые особенности закрытой структуры.
Ключевые слова: закрытая информационная структура, информационно-психологическая и педагогическая достаточность, криптографическая защита информации, инвективное воздействие.

The need for understanding the category of safety as a concept applied in various fields of knowledge – the interdisciplinary notion is studied. It aims at the characteristics of safety in the information, psychological and pedagogical perspective. It also indicates the relationships that exist between these aspects and security analysis of the closed structure, taking into account the psychological individual and group characteristics of the closed structure.
Keywords: closed information structure, psychic and pedagogical information sufficiency, cryptographic protection of information, invective influence.

Введение. В настоящее время неоспоримым является тот факт, что человек непрерывно находится в фазе информационного воздействия. Безопасность, как предмет интердисциплинарный, черпает когнитивные источники с достижений разнородных наук, в том числе психологических. С этой целью целесообразным является внедрение инструментария верификации исследуемой информации и, следовательно, вопрос обеспечения безопасности информации, а также то, каким образом данное обеспечивается. Непрерывное развитие знаний психологии, новелизация сектора безопасности является причиной расширения диапазона применения психологической и педагогической наук в дисциплинах технических. Целесообразным, в связи с этим, является рассмотрение проблематики обеспечения безопасности таких структур сквозь призму инженерно-психологического и педагогического исследования. Содержанием исследования является анализ и проектирование процессов, характеризующих субъект труда, а также исследование и разработка технических методов и средств, необходимых для этой деятельности. Объектом исследования является формирование технического аппарата методов и средств, используемых для проектирования вышеуказанных процессов.

Актуальность исследования данного направления вызвана необходимостью поиска эффективного способа формирования жизнеспособности и сопротивляемости человека в лице специалиста в отношении к угрозам внутреннего и внешнего характера – в процессе адаптации и совершенствования. Именно принятие предупредительно-профилактических мер в отношении обеспечения конфиденциальности, а также доступности информации, предотвращения утечки информации является наиболее верным подходом в создании комплексной системы информационной безопасности. Кроме того, одной из ключевых позиций играет человеческий фактор психолого-педагогического инсайдерского воздействия, что непосредственно коррелирует с обеспечением информационно-психологической защиты личности в примере работника структуры. Существенным и императивным является вопрос педагогической компетенции специалиста по защите информации. Проблема и вопрос эмоциональной регуляции целенаправленной деятельности и целостного поведения в рамках различного вида деятельности, в том числе психологической манипуляции, является условием инвективного состояния такого дискомфорта. Информационно-психологическое и педагогическое воз-

действие в проведении политики безопасности следует трактовать как целенаправленная экстраполяция информации от одного участника интеракции к другому, сопровождаемая определенными установками, оценками, восприятиями, состоянием поведения человека, на которого передача информации была акцентирована.

Негативные информационно-психологические воздействия, такие как манипулятивные влияния, влияют деструктивно на личность, сознание. Такие влияния проявляются в ипостаси инструментария психологического воздействия, давления с целью опосредованного или непосредственного, дискретного побуждения к действиям в ущерб собственным интересам в интересах отдельных лиц, групп или организаций. В рамках проведения политики безопасности следует учитывать психологические аспекты возможного воздействия при использовании методики изменения психологической и педагогической установки, а также с применением инженерно-информационной соответствующей платформы. В тоже время, такого рода психологические воздействия могут вызывать различные психические аномалии и девиации, которые могут проявляться в качестве психических расстройств и заболеваний. На человека оказывают весомое воздействие не только постоянный информационный контакт или его отсутствие, а также и эссенция, структура и качество поступающей и переработанной информации.

Информационная девиация закрытых структур. Под структурой закрытой организации понимают иерархическую структуру с определенными, однонаправленными и ограниченными отношениями «власть-подчинение», в том числе и проведения политики безопасности. Примером таких структур являются структуры информационной безопасности. Кроме иерархии в отношении «власть-подчинение» существует закрытая информационная система персональных данных, предусматривающая не только комплекс мер изолированности от внешних систем, но и возможность монополистического, административного информационно-психологическая воздействия. В таком случае возникает потребность создания концепции информационно-психологической безопасности «организация-человек» при использовании соответствующего инженерного инструментария.

Службы безопасности дипломатических структур – как структур, относящихся к категории закрытых, – являются наиболее уязвимыми с позиции обеспечения и проведения информационной политики безопасности в связи с их расположением за пределами своей страны. Данное, в свою очередь, ведет к потребности создания дополнительных защитных технических мер, а с другой стороны, имеет место быть появление эмоционального показателя инвективного воздействия на деятельность работника при принятии оперативных решений в процессе эксплуатации современных информационно-технических систем. Данное может быть вызвано существованием узкой группы лиц в пределах одной организации (25–45 человек), что может привести к фактору эмоционального профессионального «выгорания» – стрессового состояния организма, характеризующегося эмоциональным истощением, изнеможением. Симптомы такого явления и состояния проявляются постепенно, циклично. Степень выгорания характеризуется определенной комбинацией высокого или низкого уровня деперсонализации. Вся симптоматика наиболее отчетливо наблюдается на дефинитивных, необратимых стадиях, характеризующихся определенными девиациями.

Владение информацией, как технический анализ и проведение политики безопасности, включает в себя ряд приемов: информационная перезагрузка, при которой основную часть составляют абстрактные рассуждения; дозирование передаваемой информации, при котором сообщается только лимитированная часть сведений, а остальные располагаются в категории сугубо конфиденциальных, что приводит к искажению картины истинности и реальности. Пролонгация времени, как способ воздействия информацией, сводится к тому, чтобы под разнообразными претекстами откладывать обнародование истинно важных сведений до того момента и промежутка времени, когда модификация будет неактуальна, а также не будет инструментария с целью её обнаружения.

Информационно-психологические и педагогические средства обеспечения безопасности закрытых структур. Целью настоящего исследования явилось формирование концептуальных основ исследования психологической безопасности закрытой структуры, определение эссенции и предпосылок нарушения психологической безопасности с позиции

профессиональной деятельности специалистов, ядром технологии которых является возможность применения различных типов психологического воздействия, а также формирование инструментария для оценки степени риска, несоблюдение основы информационно-психологической безопасности с позиции специалистов службы безопасности. Целесообразность такой постановки проблемы обусловлена возникновением комплексных факторов, охватываемых различными источниками угроз, основная модель которых представлена следующей цепочкой: «специалист сектора безопасности – субъект безопасности – технология обеспечения безопасности структуры – корреляция специалиста сектора безопасности с субъектом». На последнем корреляционном этапе зачастую наблюдается факт возрастания информационной угрозы. Каждое лицо, как объект заинтересованности и исследования психологии, в том числе инженерной, в процессе обеспечения безопасности может быть рассмотрено в качестве участника позитивного (объект, обеспечивающий безопасность) либо негативного (объект, создающий угрозу безопасности). В двух данных случаях возможным является использование инструментария психологического с целью познания характеристик личностных, а также проведения диагностики возможных нарушений состояния психического лица исследуемого.

К исследованию проблем безопасности зачастую подходят однородно, учитывая исключительно тот факт, что защита основывается на обеспечении конфиденциальности, дискретности информации в рамках исполняемых функций. Однако не учитывается целесообразность обеспечения защиты информации от модификации, нарушения работоспособности информационной системы. В таком случае представитель службы безопасности такой «закрытой» структуры может использовать определенную закладку также деструктивного характера, в программное обеспечение, которая может передавать данные субъективно, не передавая важных технических и психологических, зачастую бихевиреальных аспектов и необходимости. Специалисты каждой службы обеспечения информации диспонируют определенной возможностью использования различных методов психологического воздействия по причине их доступности к контрольным и коррекционным технологиям.

После этого становится очевидным, что защищать, в какой области и от кого защищать. Увеличивая вероятность возникновения угрозы, формируется риск информационной угрозы. После этого можно приступать к разработке политики безопасности.

Во многих закрытых структурах существует принцип, что все прибывающие на территорию такой структуры сотрудники сдают мобильные телефоны сотруднику безопасности. Возникает дополнительный вопрос, касающийся проведения мер объективного контроля, который бы не затронул репутацию организации и не влиял на комфорт и достоинство каждого специалиста. Очевидно, следует, что это требование не является окончательно жизнеспособным, данное требование может отождествлять неэффективность информационной системы, а только лишь кажущееся, манипулятивное воздействие, компенсирующее отсутствие эффективного технического пакета и инструментария. Осознанно либо неосознанно, не регистрируя, но специалист вынужден искать альтернативные методы передачи информации, часто не предоставляющую угрозу для целой структуры. Эффективно проведенная инженерно-психологическая деятельность позволит службам осуществить выбор метода исследования и поведения по отношению к лицу, оставшемуся в радиусе заинтересованности.

Принцип информационно-психологической достаточности означает, что исследование и анализ рисков, проведенный на предварительном этапе аудита, позволяет анализировать эти риски по параметру величины и производить защиту также дополнительных аспектов. Если в качестве лимитирующего фактора выступает общее обеспечение системы обеспечения безопасности, то задачу следует решить как задачу динамического анализа и развития.

Важной является проблема психологических механизмов модификации информации в рамках ее процесса «передачи-приема». В реальном поведении часто возникают ситуации, в которых один сотрудник закрытой структуры передает в форме речевого сообщения информацию другому, которая основывается лишь на личных эмпирических выводах, зачастую субъективных. Следующий субъект, не имея возможности непосредственно контролировать объект, должен воспроизвести его. Такие задачи решаются повседневно, в том числе в струк-

турах информационной безопасности. Информационно-пропагандистские акции могут использоваться с целью укрепления авторитета источников, ввести в сомнение аутентичность такой закрытой информации.

Эмоционально негативные переживания возникают как реакции на информационную недостаточность, а зачастую дефицит. Таким образом, субъект структуры позиционирует себя событийным источником, но в тоже время его линия поведения попадает в определенную зависимость от конкретной информации. Причём, чем длиннее «цепочка», чем больше участников возникает, передаваемых информацию, не имеющих достоверной базы, тем значительнее модифицируются эти сведения.

При проведении экспериментальных исследований в пределах закрытой дипломатической мини-группы следует, что динамика таких модификаций и искажений непосредственно коррелирует с имеющимися у людей предиспозиционными факторами – субъект подсознательно настроен воспринимать в первую очередь именно то, что он ожидает. К другим причинам, способствующим возникновению и распространению псевдо-информации, относятся ограничение оперативной памяти человека, а также трудность в подборе семантических эквивалентов, постепенно вытекающая из данного подмена смысла. Также имеет место отсутствие критичного анализа, что приводит к одностороннему восприятию в сомнительных деталях получаемой информации, недостаточная оперативность, запаздывание в подаче информации.

Динамика конфликтов в информационных структурах показывает, что в настоящих условиях арсенал информационных искажений не только не сокращается, а лишь увеличивается и совершенствуется, в связи с чем человек вынужден решать вопросы технической оптимизации профессиональной деятельности, а также формирования должного эргономического обеспечения.

Техническая защита информационной безопасности закрытой структуры. В связи с существованием второстепенных факторов, влияющих на надежность передаваемой информации, важной является защита цифровых устройств от несанкционированных действий, в том числе проведение контроля представителей службы безопасности. Проведение политики инженерно-психологической корреляции минимизирует возникновение потенциального риска.

Находясь в фазе передачи пользователю, объекты интеллектуальной собственности находятся в ситуации отсутствия контроля, что может предполагать возникновение несанкционированных действий. С целью защиты персональных данных, передаваемых между информационной системой по каналам связи, выходящими за пределы контролируемой точечной фазы, необходимо использовать защищенные каналы передачи данных. При использовании таких каналов закрытых информационных систем защиты персональных данных необходимо применять средства криптографической защиты информации. Раздельно либо комплексно применяются следующие методы криптографической защиты информации: шифрование информации, фиксирование электронной цифровой подписи, как средство обеспечения подлинности электронного документа, криптографическая аутентификация как средство подтверждения санкционированного доступа субъекта к объекту, управление ключами, как необходимая составная часть систем со средствами криптографическими защиты. Необходимо установить, как должны быть защищены устройства сети, порядок использования сменных носителей информации, хранения, порядок внесения изменений в соответствующее программное обеспечение. При введении дополнительных защитных мер: использование биометрического запуска системы, использование исключительно служебной почты, применение ключа-карты в такой закрытой структуре – активность пользователей снизилась на 30 %, что связано с отсутствием точной информации, каким образом данное отображается у руководителя службы безопасности.

В критической и сомнительной ситуации, при возникновении необходимости анализа взаимосвязи используемой психологической установки с целью идентификации скрываемой информации целесообразным является проведение опроса с использованием полиграфа. В процессе данного эмпирически исследуется обоснование выбора такой установки, которая в эффекте влияет на вероятность скрываемой информации у сотрудников с разнообразными психологическими особенностями, основанными на анализе документации (рекомендаций, корреспонденции, преференций).

В процессе применения инженерно-психологических методов и средств обеспечения информационной безопасности организации закрытой структуры основой технической стороны являлось формирование средств защиты цифровых устройств от несанкционированного использования, основанным на применении физически неклонируемых функций, т. е. такой системы, которая не подлежит клонированию, имеет доступ исключительно к управленческой части системы безопасности. Наличие неклонируемых, случайных параметров делает каждую профессиональную систему уникальной и инженерно невоспроизводимой. Информация из таких контрольных систем может быть неоднократно извлечена, но в силу подачи большого количества запросов за приемлемый отрезок времени. Отпечаток пальца, как разновидность введения водяного знака, несет информацию не только о правообладателе, но и о пользователе, которому предоставляется право пользования данной копией объекта интеллектуальной оригинальной копии. Каждый водяной знак не должен присутствовать в любом цифровом устройстве явным способом, а также не должен существенным образом влиять на функционирование, аппаратные затраты и временные характеристики такого цифрового устройства. Каждая попытка удаления, модифицирования либо подмены обфускационного элемента должна быть равносильна перепроектированию системы в целостности. Такой метод является опцией шифрования данных конфиденциальных с применением секретного ключа, известного исключительно разработчику.

Внедрение любой защиты приводит к определенным неудобствам, а также игнорированию среди пользователей. Например, возможно императивно требовать проведение информационной эвиденции журнала сотрудника, в котором фиксируется время начала и конца выполнения действий, разновидность выполняемых действий, в том числе закрытых действий с точки зрения безопасности, наименование созданных файлов, учет просматриваемых страниц виртуального пространства, запрет переноса накопителей информации.

В политике безопасности закрытой структуры данный вопрос должен быть выделен в отдельный раздел. Необходимой позицией обеспечения безопасности является выделение для Интернета отдельного, автономного компьютера, на котором не должна храниться дискретная информация. При этом особый контроль надо уделить работе со сменными носителями информации, а также перлюстрации отправленной почты. В дипломатических организациях вся отправленная почта направляется вначале в руки администратора безопасности, который контролирует ее и пересылает далее соответствующим объектам. Одновременно возникает субъективный фактор владения такой личной информацией субъектов структуры представителем информационной безопасности и использование данной информации на сугубо личное усмотрение, выходящее за пределы профессионального.

В политике безопасности должны быть обязательно предусмотрены меры ликвидации этих последствий, восстановления нормальной работоспособности, минимизации причиненного сотрудником ущерба. Определенную роль играет применение средств резервирования электропитания, вычислительных средств, а также правильная организация документооборота.

Результаты вычислений и анализ. Основной целью инженерного анализа информационной безопасности является эмпирическое исследование коррелирования определенных разновидностей психологической установки и вероятности распознавания дискретной информации у лиц с различными индивидуально-психологическими особенностями, а также применение нескольких методов с целью проведения компарации полученных результатов.

С целью реализации использовалась проверка и анализ полученных результатов среди дипломатического учреждение на опрос полиграфного устройства, с другой стороны, проведены меры введения водяного знака с целью защиты информации и проведения политики безопасности, основой которой является удаление комментариев и пояснений, что является определением обфускации.

На основе классификации угроз информационной безопасности закрытой структуры по основным критериям, а именно: источник угроз, характер ущерба, вероятность и частота проявления, причины возникновения и анализа, сформирована следующая типовая структура угроз информационной безопасности закрытой структуры на примере дипломатической:

внешние возникшие угрозы и нарушения – 6 %, угрозы со стороны внешних лиц – 0,9 %, внутренние угрозы (персонал структуры) – 62 %, остальные – 30,01 %. Солидный вес занимают установка и использование нерегламентированного программного обеспечения, а также отсутствие анализа психологического воздействия в данных условиях с целью применения в личных целях, в частности, передача информации третьим лицам.

Заключение. Определены условия и возможности психологического обеспечения безопасности труда в сфере службы безопасности. Сформированы методы технической поддержки решений при проектировании эргатических систем, проведении эргономической экспертизы, определении нарушения системы безопасностями, вызванными психологическими особенностями человека в лице профессионала данного сектора.

Литература

1. Ерминек, К.Р. Информационная безопасность / К.Р. Ерминек, А. Вербицкий. – Прага : Глобальные проблемы науки, 2017. – 312 с.

2. Ерминек, К.Р. Информационная безопасность / К.Р. Ерминек // XIII Научно-техническая конференция: сб. тезисов докладов, Минск, 2–11ноября 2017 г. – Полоцк : Издат. центр Полоцкого университета, 2017. – С. 117–119.

3. Вербицкий, А. Защита информационных систем / А. Вербицкий. – Гданьск : Наука и техника, 2008. – 218 с.

4. Сулевская, А.М. Криптография в информационных системах / А.М. Сулевская. – Варшава : Защита информации, 2014. – 91 с.

Белорусский государственный университет
информатики и радиоэлектроники

Поступила в редакцию 28.01.2019