Известия Гомельского государственного университета
имени Ф. Скорины, № 2 (119), 2020

УДК 159.9:331.101.1

Инженерно-психологический анализ информационной безопасности организации и формирование педагогической компетенции операторов

К.Р. Ерминек

Исследуется необходимость понимания категории безопасности в аспекте информационном, психологическом, а также педагогическом. Содержится также анализ безопасности организации, учитывающий психологические индивидуальные и групповые особенности структуры.
Ключевые слова: криптографическая защита информации, закрытая информационная структура, информационно-психологическая и педагогическая безопасность, инвективное воздействие, педагогическая компетенция.

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

Введение. Человек, в том числе субъект профессиональной деятельности, непрерывно находится в поле информационного воздействия. Проведение политики безопасности может опираться на нескольких аспектах – проведение информационной политики, реализуемой при помощи программного инструментария, а также политики, реализуемой субъектом профессиональной деятельности, в том числе подготовки соответствующего персонала. Организации, транслирующие информационную политику, прибегают также к использованию ресурсов психологического и педагогического знания, которые исполняют и реализуют различные задания в зависимости от характера деятельности данной организации. Непрекращающееся развитие психологической и педагогической наук служит расширению возможности ее применения в функционировании информационной деятельности и среды, обеспечения информационной защиты, минимизируя при данном возможные риски на каждом сегменте реализации.

Процесс развития психологической безопасности субъекта профессиональной деятельности информационной структуры является результатом эргономического взаимодействия, процессом развития технических, производственных, системных комплексов. Каждое взаимодействие предполагает возможность наличия некоторых отклонений, вмешательств от заданного вектора.

Психологическая безопасность, также как и физическая, является независимым измерением в общей структуре безопасности, стремящаяся к нахождению физического баланса, также при этом не нарушающая аксиологические принципы, нормы субъектов в лице операторов.

В связи с непрерывным нахождением субъекта профессиональной деятельности в информационном поле, важным является проведение успешной политики информационно-психологической безопасности, как компиляция двух важных направлений – информационного и психологического. Также важным является педагогическая компетенция специалиста, реализующего защиту информации. При этом рассматривается рациональное и эффективное использование информационных ресурсов с целью защиты субъекта профессиональной деятельности от деструктивных воздействий. Под деструктивным информационным воздействием рассматриваются любые незаконные операции, связанные с доступом к информации, а также возможной ее утечкой.

На всех стадиях информационного процесса главная роль принадлежит оператору профессиональной деятельности – пользователю информации, а также ее носителю. Конечный информационный эффект зависит от соблюдения всех императивных условий передачи информации, искажения, модификации, записи, утилизации следованию принципу дискретности и последовательности, а также от психологических установок, свойств субъекта, его личностных качеств и педагогической компетентности. Инженерно-психологическую безопасность следует рассматривать как функцию нескольких переменных, состоящую из субъекта информационной безопасности, особенностей воздействия (специфики нестабильности,

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф.СКОРИНЫ

угроз), а также устойчивости к девиациям как внешнего, так и внутреннего воздействия в качестве связующего звена. Одним из источников угрозы нарушения информационной стабильности и психологической безопасности является деятельность самих субъектов профессиональной деятельности, одним из основных элементов которых является внутренняя и внешняя интеракция. В основе проведения эффективной информационной безопасности лежит недопущение компрометации в нештатной ситуации.

Информационно-психологическая неустойчивость изолированной (закрытой) структуры. Под информационной закрытой структурой понимают структуру с определенно выраженными отношениями иерархии «регулирование-реализация», а также методологией распределения информации, в том числе конфиденциальной [1]. Наглядным примером таких структур являются службы безопасности, дипломатические представительства. Кроме отношений в иерархии существует ограниченная информационная система защиты и контроля обработки и распределения персональных данных, предусматривающая комплекс изолированных мер от внешних систем, а также возможность однонаправленного, монополистического информационного воздействия. По этой причине возникает целесообразность концептуальной разработки и системы информационно-психологической безопасности типа «организация-человек» при использовании необходимого технического инструментария и информационных процедур.

Отчетливо уязвимыми и подверженными внутреннему воздействию с позиции обеспечения и проведения информационной политики безопасности являются ведомства с расположением учреждений вдали от административного источника информационной безопасности и информационного аппарата, называемой блоком центрального управления. Данное, в свою очередь, ведет к целесообразности создания второстепенных защитных мер, сегментов, а с другой стороны также имеет место возникновение суггестивного показателя, основанного на внушении, зачастую инвективным воздействием на деятельность оператора, при принятии оперативных решений в процессе приёма, переработки и выпуска информации.

Распоряжение информацией другого сегмента/блока включает в себя ряд приёмов, влияющих на целостные психологические свойства информационной структуры, в том числе: информационная перегрузка, при которой сообщается солидное количество информации, основу которой составляет сегмент дополняющий; лимитирование информации, при котором сообщается исключительно фрагментарная часть сведений [2]. Данное транслирование приводит к искажению. Возникает комбинирование истинных фактов со всевозможными гипотезами.

Психологические и педагогические установки в обеспечении информационной безопасности. Проблема информационно-психологической безопасности субъекта профессиональной деятельности и ее решение определяют необходимость обеспечения такого рода безопасности личности в применении соответствующего методологического аппарата. Без константного информационного контакта невозможным является динамическое развитие как организации, так и субъекта деятельности. При этом остается факт содержания в себе прогрессирующих угроз для развития личности в лице профессионала. Современный уровень исследования проблематики информационной безопасности и обеспечения на соответствующем уровне характеризуется, с одной стороны, отсутствием акцентирования связующего звена «работник-безопасность», с другой стороны, изучением проблематики безопасности личности и ее различных аспектов в качестве независимого направления. Необходимым является проведение аудита информационных процессов организации, интервьюирование операторов, выявление критически важной информации, которая находится в рамке защиты. Зачастую данное рассматривают однонаправленно, утверждая, что защита заключается исключительно в обеспечении дискретности информации. При этом не рассматривается необходимость обеспечения защиты информации от угроз нарушения работоспособности системы. В качестве примера, представитель службы безопасности такой закрытой структуры может воспользоваться введением программного фрагмента, который передаёт данные однородно, не передавая технические важные параметры и не учитывая психологическую особенность восприятия такой модели передачи информации.

В большинстве случаев в качестве нарушителей позиционируют – произвольно либо непроизвольно – субъекты профессиональной деятельности. Существенным также является вероятность и частота такого характера реализации угроз.

Например, в политике безопасности может быть регламентировано, что все прибывающие на территорию такой структуры сдают средства внешнего информационного доступа, за-

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

поминающие устройства сотруднику безопасности и контроля. При этом отсутствуют технические альтернативы сканирования, нелегального переноса в организацию. Единственным источником контроля является проверка личных вещей сотрудников в непланируемые дни. Возникает альтернативный вопрос, касающийся проведения мер объективного контроля, который бы не затронул реноме персонала, его психологическое состояние и психологический климат организации в целом. Очевидно, что это требование не является окончательно исследуемым.

Принцип информационной достаточности означает, что затраты на обеспечение безопасности информации должны быть соизмеримы с потенциальным ущербом и рисками, в том числе психологическими. Анализ потенциальных рисков, проведенный на первоочередном контрольном этапе, позволяет ранжировать такие риски по значимости и обеспечивать защиту участков, первоначально обрабатывающих наиболее важную информацию.

Одной из ключевой является проблема психологических рычагов трансформации информации в процессах «передача-прием». В ежедневном поведении зачастую осуществлять контроль за технически-информационным состоянием предмета, применяя не только информационно-технический ресурс, но также и субъективное наблюдение. В дальнейшем информация воссоздаётся на основании, в том числе, совокупности элементов такого образа, основанного на восприятии сообщения. Данное находит практическое применение в фазе непрерывного информационного воздействия безопасности, что может использоваться с целью усиления позиции распространителей, формирования сомнения в аутентичности передаваемой закрытой информации.

Эмоциональные переживания негативного характера возникают как реакция на информационный дефицит и авторитетное воздействие, характеризующее ранжированием профессионального статуса, возможных действий. Таким образом, субъект структуры ощущает себя информированным, но при этом поведение объективно начинает попадать в радиус зависимости от информации. Чем более протяженной является длина и количество элементов, тем большее количество принимает участие в экстраполировании сведений, не обоснованных достоверными данными официальных источников информации, тем более модифицируются данные сведения.

Актуальным является экстраполяция ликвидации информационных проблем на предупреждение таких отклонений, что актуализирует необходимость формирования педагогической компетенции специалиста. Такая профессиональная компетентность оператора выражается в способности транслировать воздействие на развитие личностных и ценностных параметров субъектов профессиональной деятельности, прогнозировать и ликвидировать нежелательные проявления в поведении персонала.

При проведении экспериментальных исследований в пределах закрытой информационной группы Варминско-Мазурского Университета (110 субъектов профессиональной деятельности) следует, что характер этих искажений непосредственно коррелирует с имеющимися у операторов информационно-психологическими установками, что связано с подсознательным восприятием ожидаемой информации. К объективным причинам внедрения иного характера, способствующим распространению квази-информации, относятся следующие психологические факторы: ограничение оперативной памяти оператора, специалиста, трудности подбора точных дефиниций событий, фактов; «дополнение» фрагментов отсутствующей информации, что приводит к такому восприятию информации, при котором априори не возникают второстепенные вопросы в деталях получаемой информации, вызывающие долю сомнения.

Развитие информационных конфликтов в структурах показывает, что в актуальных условиях арсенал информационных деформаций и нарушение политики безопасности при проведении психологических операций динамически развивается.

Информационные процедуры как установка обеспечения информационно-психологической безопасности закрытой структуры. С целью изучения особенностей коррелирования психологической установки и вероятности распознавания дискретной информации используется полиграфный метод. Целесообразным является применение смены психологических установок опрашиваемого специалиста, в том числе представителей службы безопасности, что повысит вероятность распознавания информации. На предварительном этапе проведен анализ педагогических компетенций, связанные с профилактическими действиями отклоненного поведения, основанный на проектировании внешних и внутренних уязвимостей, а также формированием мотивирующих факторов и среды. Оценка полученных результатов производилась при помощи технического обеспечения SRS Femida, алгоритма математической обработки полученной информации, корреляционно-регрессионного анализа методов технического анали-

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф.СКОРИНЫ

за. В процессе проведения эмпирического этапа апробирован инструментарий исследовательского характера, основанный на согласовании определения психологической установки, выявления критериев, а также определения аутентификации скрываемой информации [3].

Изучены взаимосвязи между занимаемым рангом каждого профессионала, его индивидуальными особенностями, в том числе психологического, в процессе полиграфного опроса, применяя адаптационные тестирующие установки, основанные на ложные ответы, правдивые, также в сочетании с позитивным контролем. Такие сменные методики позволяют проводить детекцию закрытой структуры на основе комплексно-методологического контроля.

Также применяются средства защиты технического характера: шифрование как средство обеспечения конфиденциальности информации, электронная цифровая подпись в качестве верификации подлинности документа, аутентификация в качестве подтверждения санкционированного доступа субъекта к объекту, управление ключами как необходимая составная часть систем со средствами защиты информации с целью изготовления, хранения и уничтожения ключевых элементов, введение биометрических систем аутентификации оператора. После внедрения биометрического способа активизирования работы систем (введение отпечатков пальца сотрудников), а также повторного проведения детекции, обнаружено, что попытки нарушения проведения политики безопасности снизились на 20 % (согласно проведению опросов), что свидетельствует о положительном эффекте введения предупредительно-защитных технических мер, а также обнародованию такой информации.

Внедрение технической защиты может привести также к определенному психологическому дискомфорту пользователя. Однако эти неудобства не должны оказывать первоочередного, доминантного влияния, иначе будет непосредственно либо опосредованно игнорированы существующие императивные в пределах данной информационной системы правила [4]. Особый контроль надо уделить работе со сменными носителями информации, а также анализу высылаемой почты. В закрытых информационных системах вся входящая/исходящая почта попадает к эксперту центрального блока безопасности, который осуществляет выборочный контроль и пересылает данные далее. Вместе с данным возникает дополнительное, зачастую субъективное, владение информацией субъектов структуры представителем информационной безопасности и индивидуальное использование данной информации.

Одним из этапов является выявление и систематизация ошибок операторов в результате несовершенствования технических процедур.

Заключение. В политике безопасности изолированной структуры императивным является предусмотрение мер ликвидации последствий владения информацией и восстановление нормальной работоспособности, минимизации причиненного ущерба. Приведены результаты исследования эффективности использования методики инженерно-психологической установки в обеспечении информационной безопасности закрытой структуры, а также взаимосвязи психологической установки и распознавания скрываемой информации при использовании технических методов, являющихся трудно воспроизводимыми и имитируемыми. Обоснована сущность педагогической компетенции специалиста в лице оператора, непосредственно связанная с уязвимостью информационной безопасности в отношении к уровню компетенции. Исключительно учитывая комплексные факторы психологического взаимодействия, можно сформировать эффективную информационную систему.

Литература

1. Ерминек, К.Р. Информационная безопасность / К.Р. Ерминек, А. Вербицкий. – Прага : Глобальные проблемы науки, 2018. – 209 с.

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

3. Вербицкий, А. Защита информационных систем / А. Вербицкий. – Гданьск, 2007. – 215 с.

4. Сулевская, А.М. Криптография в информационных системах / А.М. Сулевская. – Варшава : Защита информации, 2016. – 125 с.

Белорусский государственный университет
информатики и радиоэлектроники

Поступила в редакцию 19.12.2019

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ