УДК 681.3.07

МЕЖЛИЧНОСТНЫЕ ПСИХОЛОГИЧЕСКИЕ ОТНОШЕНИЯ В АСПЕКТЕ ЭФФЕКТИВНОСТИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Валерий Слепцов, Владимир Журавлев
Запорожский национальный технический университет

Анотація: **Розглядаються питання впливу міжособових відносин в диференційованому середовищі користувачів інформаційних систем на стан їх захисту.**
Annotation: **The questions of influence of individual relations in derivative society of information systems users on their safeguard status are under review.**
Ключевые слова: **Политика информационной безопасности, психологические отношения, источник угроз, психологические типы личности.**

I Введение. Постановка задачи

В Запорожском национальном техническом университете для студентов специальности «Защита информации от несанкционированного доступа» читается курс лекций по дисциплине «Психология экстремальных ситуаций», в котором, в числе прочих вопросов, рассматривается влияние психологической подготовки коллектива на эффективность реализации политики безопасности предприятия. Одним из аспектов психологической подготовки является формирование межличностных отношений сотрудников, являющихся пользователями и носителями информации с ограниченным доступом, в расчете на создание условий, исключающих неконтролируемое распространение такого рода информации со стороны персонала, а также обеспечивающих целостность и доступность информационных ресурсов.

Как известно [1], политика безопасности информационных систем предприятия обеспечивается путем реализации комплекса правовых, организационных и программно-технических мер, позволяющих нейтрализовать угрозы потенциального противника или уменьшить вероятность их реализации до заданной величины. В ряду организационных мер защиты информации особое место занимает идеологическая (с позиции политики безопасности) и психологическая работа первых руководителей предприятия, направленная на минимизацию негативного влияния человеческого фактора (поведение индивида в обществе) на вероятность реализации угроз противника. Человеческий фактор является, в ряде случаев, причиной и движущей силой нарушений или преступлений со стороны всех категорий пользователей информационной системы, являющихся, с одной стороны, – ее необходимым элементом, а с другой – потенциальным источником угроз. Создают, получают, обрабатывают, хранят информацию, обеспечивают ее конфиденциальность, целостность и доступность исполнители, поэтому они являются наиболее ответственным и уязвимым объектом системы защиты информации.

Роль человеческого фактора так же определяется высокой степенью психологической неопределенности поступков конкретного индивида во времени и в конкретной обстановке, непредсказуемостью их возможных мотивов, коррелированных с его личностными характеристиками и условиями контакта в среде обитания. Характер и вероятность реализации угроз со стороны персонала определяются, следовательно, рядом психологических факторов, которые являются предметом исследования многих авторов, занимающихся проблемами обеспечения информационной безопасности (ИБ) [1, 2].

Одним из таких факторов является характер межличностных отношений в среде сотрудников, имеющих доступ к защищаемой информации с установленным объемом полномочий. Достаточно хорошо изучена природа межличностных конфликтов, степень их влияния на эффективность работы персонала [3]. Однако, по мнению авторов, влиянию человеческого фактора в межличностных отношениях на обеспечение информационной безопасности уделяется недостаточное внимание. В статье предложены методы оценки воздействия межличностных конфликтов исполнителей, занимающих различные уровни служебной иерархии, на состояние политики ИБ предприятия.

II Основная часть

Каждое предприятие разрабатывает политику ИБ, формирует социально-психологический климат в коллективе, имея в виду не только создание условий для повышения эффективности производственной деятельности, но и устранение причин для возникновения конфликтов в своих подразделениях, несущих угрозы для этой деятельности. Межличностные отношения в среде пользователей и распорядителей

системных информационных ресурсов, определяющие возможность возникновения конфликтов, безусловно, оказывают непосредственное влияние на состояние политики ИБ.

Различают три уровня конфликтов [2].

Внутриличностный конфликт, в основе которого лежит несогласие индивида-исполнителя, основанное на его воззрениях, с принимаемыми руководителями управленческими решениями.

Межличностный конфликт, под которым понимается ситуация, в которой его субъекты (два или более) отвергают полностью или частично позицию оппонента. То есть, в основе любого межличностного конфликта лежит расхождение мнений участвующих в нем сторон по поводу стратегии или тактики выполнения поставленных задач. Принимая межличностные конфликты как неизбежный процесс творческого подхода исполнителей к решению поставленной задачи, необходимо отметить, что не всякий конфликт можно рассматривать, с позиции руководителя, как негативное явление. Позитивные результаты некоторых конфликтов состоят в том, что они побуждают исполнителей к анализу различных тактик достижения цели, оптимизации методов и устранению технических либо организационных ограничений, мешающих качественной реализации поставленной задачи. В дальнейшем будем анализировать только негативное воздействие участников конфликта на эффективность реализации политик ИБ.

Причинами межгруппового конфликта чаще всего являются различные подходы формальных и неформальных групп исполнителей к решению задач, преданность интересам группы и борьба за ресурсы.

Очевидно, что задача менеджмента ИБ заключается в организации процесса управления конфликтами с достижением цели - предотвращения либо погашения конфликта с минимальным ущербом для участников информационных отношений и ИБ предприятия. В любых межличностных отношениях человеческий фактор выступает как совокупность объективных условий (предпосылок) психического, социально-экономического, политического, идеологического, морального, национального, природного и техногенного характера, действующих в данное время и данном пространстве и обусловливающих негативное или позитивное поведение человека и его поступки [4]. Конечно, это не означает, что все предпосылки действуют одновременно, все сразу. Информация похищается, уничтожается, модифицируется при различных обстоятельствах и по разным причинам. В одном случае исполнитель может действовать по политическим, идеологическим и национальным мотивам. В другом случае его действия обусловлены социально - экономическими и моральными проблемами, в следующем – только психическими.

Рассматривая психические мотивы, можно выделить 7 типов личности, поведение которых, представляет угрозу ИБ предприятия [5].

4. Аддитивное поведение. Уход от реальности путем изменения своего психического состояния – с помощью наркотиков, алкоголя или постоянной фиксации внимания на определенных предметах или видах деятельности (карты, лотерея, женщины и т. д.) для получения интенсивных эмоций. Эти процессы во многом управляют жизнью человека, делают его беспомощным, лишают воли. Для достижения своих целей исполнитель с аддитивным поведением (аддикт) может пожертвовать многим, если не чем угодно.

5. Антисоциальное поведение. Основная черта – совершение действий, противоречащих этике и морали, безответственность, игнорирование законов и прав других людей.

6. Суицидное поведение. Подвергающее свою (соответственно и рядом находящихся исполнителей) жизнь риску.

7. Конформистское поведение. Исполнение воли «авторитета», приспособленчество, не критичность, неспособность принимать решения, брать на себя ответственность.

8. Нарцисстическое поведение. Повышенная чувствительность к оценкам других людей, отсутствие достаточного чувства сопереживания, дистанцирование от коллектива (как следствие не приятие его социальных и этических норм и требований).

9. Фанатическое поведение. Слепая приверженности какой-либо идее, нетерпимость к другим взглядам, что может сопровождаться действиями насильственного характера. Нейтральные или дружеские поступки других людей часто оцениваются как враждебные или, заслуживающие презрения.

10. Аутистическое поведение. Затруднение социальных контактов, оторванность от действительности, погруженность в сферу мечтаний. Отсюда невозможность адекватно оценить ситуацию и принять решение.

Названные типы личности формируют негативное состояние социально-психологического климата в коллективе, осознанно или неосознанно провоцируют в нем межличностные конфликты, противодействуя тем самым (как один из факторов) реализации политики лоялизации персонала. Степень информационной надежности исполнителя зависит от разных причин и может меняться в связи с изменением условий, возникновением нестандартных и особенно экстремальных, кризисных ситуаций. В этих ситуациях весьма вероятно проявление информационной ненадежности у тех людей, которые не считают нужным соответствовать моральным требованиям или же обладают некоторыми личностными недостатками,

характер которых приведен выше.

Рассмотрим возможное влияние психологических особенностей различных типов пользователей автоматизированной системы обработки информации (АСОИ) на состояние ее защищенности в зависимости от уровня конфликта. Используя приведенную выше классификацию типов "конфликтных" личностей, можно составить схемы, позволяющие наглядно показать зависимости типа – служебное положение-личность-угроза.

Для внутриличностных конфликтов такая схема в применении, например, к системному администратору, по мнению авторов, может иметь вид, представленный на рис. 1.

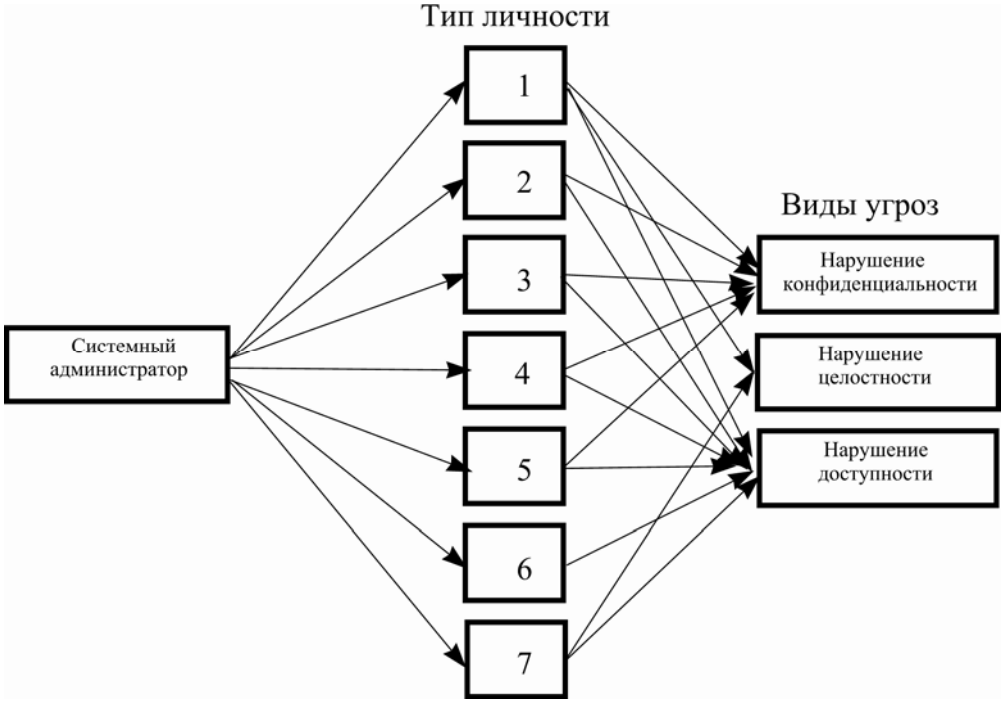

Рисунок 1 – Влияние психологических особенностей различных типов пользователей на состояние защищенности системы в зависимости от уровня конфликта

Приведенные взаимосвязи основываются на возможностях доступа системного администратора к информационным ресурсам и уровне его стандартных полномочий. По аналогичному принципу можно составить подобные схемы и для других категорий пользователей (администратор безопасности, администратор баз данных, пользователь-программист и т. д.), беря за основу их права доступа и уровни полномочий. Очевидно, что учет психологических особенностей сотрудников, осуществляющих работы с защищаемой информацией, предоставляет возможность построить гораздо более точную модель внутреннего нарушителя конкретной АСОИ.

Более сложный характер будут иметь взаимосвязи подобного рода при исследовании влияния типов личностей на возникновение угроз ИБ при межличностных и межгрупповых конфликтах. В этих случаях следует учитывать не только психологические характеристики личностей, но также характер и степень их возможного влияния на процесс делового взаимодействия и общения. При этом необходимо предусмотреть возможность несовпадения целей, стоящих перед различными исполнителями и конфликтующими группами. По-видимому, наиболее эффективный метод исследования таких взаимосвязей – идти от частного к общему. То есть, используя психологический портрет личности потенциальных участников межличностных конфликтов, оценивая степень их возможного влияния на те или иные функции политики безопасности в процессе делового сотрудничества, получить обобщающие данные, позволяющие охарактеризовать социально-психологический климат в коллективе пользователей АСОИ. На основе таких данных можно выработать рекомендации, направленные на предотвращение конфликтов, сулящих конкретные угрозы системной безопасности.

Идти, по-видимому, надо от исследования влияния критичных (с точки зрения обеспечения ИБ) парных связей между отдельными категориями пользователей АСОИ, постепенно усложняя задачу. Например, для оценки рисков функционирования системы разграничения доступа наиболее важным представляется

сопоставление психологических характеристик личностей системного администратора и администратора безопасности. Результаты такого сопоставления, дающие основания сделать вывод о высокой вероятности их несовместимости, а значит, предрасположенности к межличностному конфликту, предполагают принятие адекватного ИБ управленческого решения. На рис. 2 показана зависимость степени риска для системы разграничения доступа к информационным ресурсам АСОИ от типов личностей (выбраны три потенциально опасные категории), осуществляющих функции администрирования.

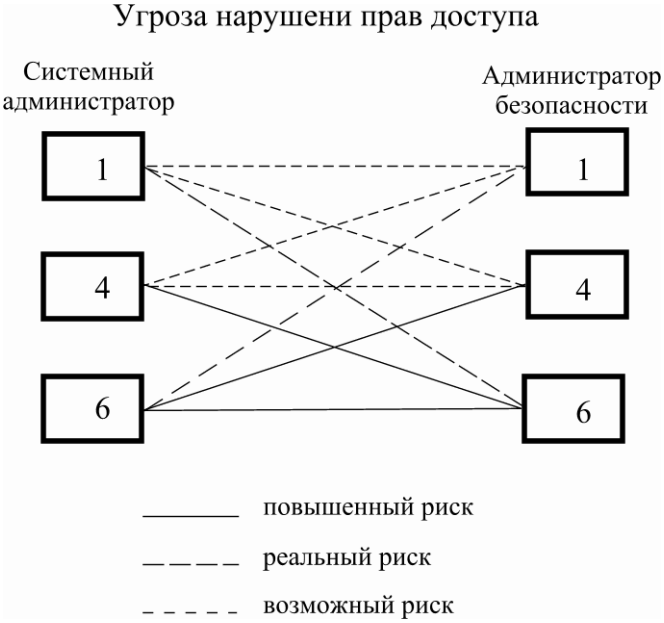

Рисунок 2 – Угроза нарушения прав доступа

Очевидно, что предлагаемый подход к оценке влияния психологических качеств личности на защищенность АСОИ наиболее эффективен при решении вопроса о возможности устройства на работу того или иного кандидата, который будет иметь дело с конфиденциальной информацией. При организации работы в уже сформировавшемся коллективе пользователей необходимо учитывать ряд других факторов, определяющих поведение сотрудников. Это, прежде всего, действия администрации, которые направлены на формирование мотивационных побуждений персонала и способствующие достижению требуемого уровня ИБ, а также состояние режима безопасности.

III Выводы

Рассматривая человеческий фактор как один из основных для обеспечения защищенности АСОИ, важно учитывать влияние психологической характеристики пользователей с точки зрения возможного проявления своеобразия качеств отдельной личности на состояние межличностных отношений, а, следовательно, и на уровень защищенности информационных ресурсов. Такие зависимости желательно прослеживать не только для предупреждения утечки информации ограниченного доступа, но и для обеспечения ее целостности и доступности. Особое внимание следует обращать на те личностные качества, которые определяют отношение сотрудника к:

- выполнению регламентных требований;
- выполнению указаний руководства в области обеспечения ИБ;
- негативному воздействию со стороны внешней и внутренней среды;
- способу оценки, как своих действий, так и действий коллег по работе;
- вредным привычкам;
- форме и способе отстаивания собственного мнения;
- необходимости учета интересов других лиц в процессе делового и неформального общения и т. д.

При осуществлении мероприятий, направленных на развитие корпоративной культуры и предупреждение или нейтрализацию угроз со стороны персонала в области ИБ, вопросу изучения психологических качеств сотрудников, имеющих дело с защищаемой информацией, следует уделять внимание на всех этапах кадровой работы: подбор кандидатов, проверка и изучение потенциальных

сотрудников, выдвижении на должность, организация контроля, увольнение. Поскольку методика изучения и оценки психологии личности – прерогатива специалистов соответствующего профиля, в основу этой работы должна быть положена деятельность профессиональных психологов при обязательном участии сотрудников кадрового аппарата, службы безопасности, руководителей подразделений. Затем, на основе сопоставления психологических портретов пользователей, участвующих в информационном обмене, с учетом характера их взаимодействия следует оценить риски возникновения межличностных конфликтов, способных негативно повлиять на состояние ИБ. Построенная таким образом работа с персоналом позволяет:

- предотвратить межличностные конфликты;
- своевременно выявить признаки назревающих конфликтов;
- принимать адекватные меры, направленные на решение конфликтов и устранение условий, способствующих их созреванию;
- минимизировать риски в области ИБ, определяемые человеческим фактором.

Изучение вопросов, рассмотренных в настоящей работе в рамках указанной выше дисциплины, обеспечивает необходимую разноплановость в подготовке специалистов и магистров в области защиты информации и позволяет дать им практические рекомендации, реализация которых в их будущей деятельности положительно скажется на уровне обеспечения ИБ объекта информационной деятельности.

Литература: ***1.*** *Духов В. Е. Экономическая разведка и безопасность бизнеса. - Киев: ИМСО МО Украины, НВФ "Студцентр", 1997. – 175с.* ***2.*** *Пюкке С. М. Конфликтное социальное взаимодействие в информационной сфере // Сб. научн. тр. "Інформаційні технології та безпека". Вип. 5, Институт проблем регистрации информации НАН Украины, Киев, 2003. С. 58-69.* ***3.*** *Нюстром Джон В., Дэвис К. Организационное поведение: поведение человека на рабочем месте. - Сп.Б., 2000.* ***4.*** *Гаврюшин Е. И. Человеческий фактор в обеспечении безопасности конфиденциальной информации: http//www.it2b.ru/it2b3.view1.page3.html.* ***5.*** *Прасолов В. И. Технологии обеспечения лояльности персонала в структуре политики безопасности фирмы. Материалы конференции: "Создание системы корпоративной безопасности. Практические подходы", Москва, 2005: http://www.it2b.ru/it2b2.view6.page32.html*

УДК 681.3.06

КОНЦЕПЦІЯ ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО РЕЖИМУ КОНТРОЛЮ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ

Ігор Терейковський
Державний університет інформаційно-комунікаційних технологій

Анотація: **Запропонована концепція визначення оптимального режиму контролю атак на комп'ютерні системи. Основою концепції є використання параметрів, що визначають технічний стан об'єкта захисту та модель оптимізації режиму контролю, адаптована до захисту від атак на відмову в обслуговуванні. Використання даної концепції доцільне при формуванні систем аналізу захищеності та систем виявлення атак.**

Summary: **The concept of definition of an optimum verification mode of attacks on computer systems is offered. By a basis the concept is use of parameters, which define a technical status of object of protection and model of optimization of a verification mode adapted to protection against attacks on failure in service. Use of the given concept is expedient at formation of systems of the analysis of security and systems of definition of attacks.**

Ключові слова: **Атака на відмову в обслуговуванні, оптимальний режим контролю, об'єкт захисту, система виявлення атак, система аналізу захищеності.**

I Вступ

Для більшості вітчизняних та закордонних організацій ефективність функціонування багато в чому залежить від надійної та ефективної роботи їхніх комп'ютерних систем. При цьому однією із досить давніх та основних проблем забезпечення надійної та ефективної роботи корпоративних комп'ютерних систем є проблема безпеки інформації, що циркулює та зберігається в цих системах. Відзначимо, що з поширенням використання локальних комп'ютерних мереж та глобальної мережі Інтернет вказана проблема набуває все більшої актуальності, адже комп'ютер, підключений до мережі, може бути