ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЧЕЛОВЕКА И ОБЩЕСТВА В ЭКСТРЕМАЛЬНЫХ СИТУАЦИЯХ

НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ КУЛЬТУРЫ

А.В. Богданов, кандидат технических наук, доцент;
И.Г. Малыгин, доктор технических наук, профессор;
Ю.И. Синещук, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены проблемы формирования модели нарушителя как основного способа повышения эффективности функционирования системы безопасности. Проанализированы основные побудительные конфликты, направления деятельности руководства и службы безопасности по их смягчению.

Ключевые слова: нарушитель, угрозы безопасности, модель нарушителя, безопасность.

INFORMAL MODEL OF THE VIOLATOR OF SECURITY CULTURE OBJECT

A.V. Bogdanov; I.G. Malygin; Yu.I. Sineshchuk.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The problems of forming of model of violator are examined, as a basic method of increase of efficiency of functioning of the system of safety. Basic incentive conflicts, directions activity of guidance and service safety, are analysed on their softening.

Keywords: violator, threats a without-danger, model of violator, safety

Объекты культуры, крупные музейные комплексы как любая сложная развивающаяся структура предъявляют к организации систем безопасности различные и часто противоречивые требования. Предлагаемые сегодня концепции безопасности, являясь несомненно полезными и выверенными, с точки зрения охраны, как правило, не учитывают музейную специфику и предполагают рассмотрение проблемы как проблемы информационно-технической, обеспечивающей не только интересы и структуру безопасности как таковую, но и взаимосвязь ее с социологической организацией колллектива, интересы как посетителей, так и работников музея. Большое число гостей музея и работающих сотрудников находятся в музейном комплексе испытывая на себе влияние различных факторов, среди которых все большую роль начинают играть вопросы безопасности [1].

Вопросы безопасности такого рода систем часто сводятся к вопросам человеческих отношений и человеческого поведения (рис. 1).

Проводя анализ нарушений информационной безопасности, особое внимание следует уделять не только самому объекту нарушения, но и личности нарушителя, то есть субъекту нарушения. Это поможет разобраться в мотивах преступления и даст возможность избежать повторения подобных ситуаций [2, 3].

Нарушителем безопасности называют лицо, которое осуществляет запрещенные законом и правилами действия, либо по ошибке, либо по незнанию, либо осознанно. Наиболее опасен – злоумышленник как разновидность нарушителя, который намеренно идет на преступление из корыстных побуждений.

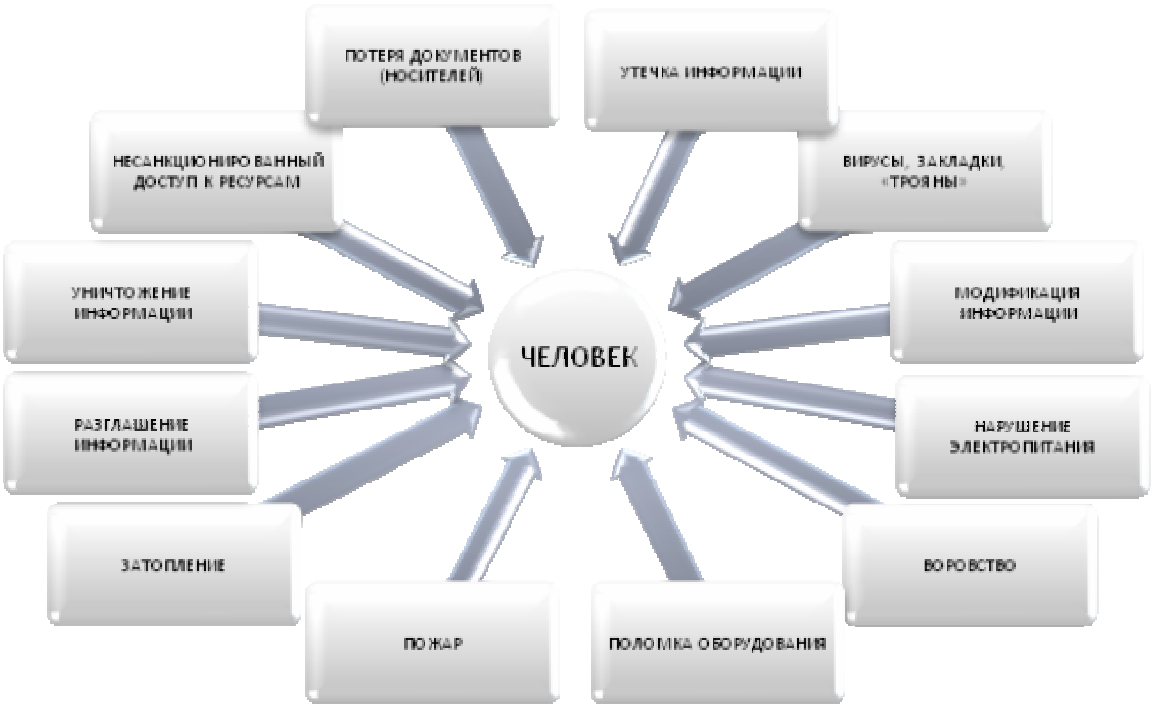

Рис. 1. **Роль человеческого фактора в реализации угроз безопасности**

В общем случае нарушитель может быть внешним по отношению к защищаемой системе (посторонние лица) и внутренним (из числа персонала), пользователь – в широком смысле.

Особую сложность в профилактике и раскрытии преступлений представляют именно пользователи, с одной стороны, это ее необходимый элемент, а с другой стороны – источник нарушения или преступления. Поэтому целесообразно заблаговременно построить модель нарушителя безопасности, которая характеризует его знания, навыки, время и место действия и т.п. [4].

Построения концептуальной модели нарушителя целесообразно начинать с анализа социальных истоков преступности. При этом надо учитывать, что между людьми часто возникают конфликты (рис. 2), которые могут сказаться на состоянии безопасности.

Анализ сути и содержания социально-психологических конфликтов позволяет выработать конкретные рекомендации, позволяющие воздействовать и даже управлять социально-психологической обстановкой в коллективе, способствуя тем самым повышению уровня защищенности объекта [5].

Рис. 2. **Основные типы конфликтов в сфере безопасности**

Суть типовых конфликтов заключается в следующем:

– Требования режима заставляют искать возможность компенсации неудовлетворенных потребностей, отрицательно влияют на психофизиологические и профессиональные качества сотрудников, негативно переживаются сотрудниками, а зачастую приводят к игнорированию последних.

– Ограниченность ресурсов приводит к конфликту и между отделами, и между сотрудниками, способствует появлению служебных интриг.

– Несоответствие целей. Инструментальный конфликт возникает из-за подмены главной цели, поскольку функции службы безопасности (СБ) носят вспомогательный (обслуживающий) характер.

– Психологические. Контролирующие функции СБ раздражают специалистов (пользователей). Синдром ответственности проявляется в прогнозировании и негативном переживании возможных неблагоприятных последствий той или иной служебной ситуации.

– «Несбывшиеся надежды» – конфликт неудовлетворенности потребностей, целей (карьера, условия работы, зарплата, успех, призвание и др.).

Иерархические. Существуют четыре вида конфликтов иерархии:

«равный-равный»;

«высший-низший»;

«высший-средний-низший»;

формальной и неформальной структур, который может привести к борьбе за власть в различных формах.

– «Человек-машина». Характеристики технических средств должны удовлетворять возможностям человека.

– В личной жизни – неурядицы в отношениях с близкими людьми.

Предложенная классификация позволяет в каждом конкретном случае выявить негативные последствия конфликтов и обосновать рекомендации по их предотвращению.

Выделяют три основные побудительные причины нарушений информационной безопасности со стороны пользователей: безответственность, самоутверждение, корыстный интерес.

В первом случае пользователь осознанно или случайно осуществляет какие-либо деструктивные действия, не связанные со злым умыслом. Как правило, это является следствием его некомпетентности или небрежности.

Отдельные пользователи рассматривают доступ к ресурсам своим достижением, ведя своеобразную игру ради удовлетворения собственных амбиций либо самоутверждения в глазах коллег. При этом их намерения могут быть и безвредными. Пользователи с более агрессивными намерениями могут осуществить попытку испортить или уничтожить объекты системы. В этом случае говорят о зондировании системы. Самоутверждаясь, нарушитель умышленно воздействует на систему, зондирует ее. Такое поведение может быть вызвано обидой, неудовлетворенностью служебным или материальным положением или осуществляться по указанию других лиц.

Нарушение безопасности может быть спровоцировано и корыстным интересом. В этом случае нарушитель будет целенаправленно стараться обойти систему безопасности для осуществления доступа и воздействия на объекты.

Опыт показывает, что частота того или иного вида нарушений обратно пропорциональна наносимому им ущербу: чаще всего встречаются нарушения, вызванные халатностью и безответственностью, ущерб от них незначителен и легко восполняется. Ущерб от зондирования системы, как правило, больше, но вероятность его реализации ниже, поскольку требует достаточно высокой квалификации, знания особенностей системы защиты и наличия определенных психологических особенностей. При этом размер ущерба прямо пропорционален положению пользователя-нарушителя в служебной иерархии.

Наиболее редким, но и наиболее опасным видом нарушения является проникновение. Его отличием обычно является определенная цель – доступ к определенным объектам, нарушение функционирования комплекса, контроль и дезорганизация действий других пользователей и др. Для осуществления проникновения нарушитель должен обладать теми же качествами, что и для зондирования системы, но в более совершенном виде. В силу этих обстоятельств ущерб от этого вида нарушений часто бывает невосполнимым.

Способы предотвращения нарушений вытекают из природы побудительных мотивов. В качестве базовых профилактических мер можно назвать подготовку пользователей, поддержание здорового климата в коллективе, подбор персонала.

Сочетание этих мер дает возможность не только устранять нарушения и проводить эффективное расследование преступления, но и предотвращать саму их причину.

Описанные особенности нарушителей следует рассматривать как предрасположенность к совершению преступления. Однако реализация этой предрасположенности зависит от личности пользователя, ее ценностных ориентаций, складывающихся под влиянием социальных отношений, в которые он включен.

Модель нарушителя позволяет выявить условия, при которых может произойти формирование психологической готовности к противоправным действиям и произвести общую типизацию криминальности потенциального нарушителя [5]:

– первый тип обусловлен наличием определенной криминальной потребности (получаемый результат и сами преступные действия – процесс их совершения);

– второй тип обусловлен принятием преступного способа удовлетворения потребностей или разрешения проблемной ситуации как более предпочтительного, по сравнению с правомерным или совместно с использованием правомерного;

– третий тип обусловлен принятием преступного способа удовлетворения потребностей лишь при благоприятных условиях, предоставляющих не только возможность получения результата, но и максимальную скрытность;

– четвертый тип обусловлен внутренне противоречивым (вынужденным) принятием преступного способа действий (например, когда, по мнению субъекта, отсутствует возможность правомерного достижения результата, но при этом остается необходимость его получения);

– пятый тип обусловлен склонностью к импульсивному совершению преступных действий как реакции на определенные ситуации;

– шестой тип обусловлен принятием преступного способа действий под криминогенным воздействием третьих лиц.

Каждый тип нарушителя должен быть охарактеризован значениями соответствующих характеристик. При этом необходимо помнить, что определение конкретных значений характеристик модели нарушителя в значительной степени субъективно и, следовательно, модель нарушителя может быть представлена перечислением нескольких вариантов его облика.

В процессе разработки модели нарушителя необходимо определить:

– категории лиц, к которым может принадлежать нарушитель;

– мотивы действий нарушителя (его цели);

– квалификацию нарушителя, его осведомленность о системе защиты и оснащённости;

– характер возможных действий нарушителя.

При этом необходимо учитывать следующие факторы:

– хорошо поставленная работа по подбору кадров и профилактические мероприятия препятствуют формированию коалиций нарушителей, их сговора;

– принцип «враждебного окружения» предполагает, что любой нарушитель скрывает свои преступные действия от других сотрудников;

– деструктивные проявления в функционировании объекта защиты могут быть следствием элементарных ошибок сотрудников (пользователей, администраторов, эксплуатирующего и обслуживающего персонала), а также недостатков принятой технологии обработки информации и т.д.

Исходя из рассмотренных положений, «модель нарушителя», адекватная реальным возможным типам нарушителей включает описания его практических и теоретических возможностей, место и время реализации его действий, другие характеристики [5, 6]. Такая модель может служить основой прогнозного сценария реализации криминальных поступков, позволяет проанализировать причины нарушений и дает возможность либо устранить их заблаговременно, либо обоснованно сформулировать требования к разрабатываемой системе защиты и эффективно проводить мероприятия по профилактике и расследованию преступлений.

Литература

1. Богданов А.В., Краснов А.В. Информационная система обеспечения безопасности крупных музейных комплексов // Пожаровзрывобезопасность. 2007. № 1.

2. Компьютерная преступность и информационная безопасность / под ред. А.П. Леонова. Минск: Арил, 2000. 377 с.

3. Примакин А.И., Синещук Ю.И., Пантиховский О.В. Правовые аспекты безопасности единого информационного пространства силовых ведомств (МВД, МЧС, МО) // Вестн. С.-Петерб. ун-та МВД России. 2012. № 2. С. 234–240.

4. Козьмовский Д.В., Куватов В.И., Пантиховский О.В. К вопросу о классификации деятельности пользователей в распределенных сетях: тр. XII С.-Петерб. междунар. конф. «Региональная информатика (РИ-2010)». СПб.: СПОИСУ, 2011. С. 157–160.

5. Статьи об информационной безопасности: [сайт]. URL: http://www.Avoidance.ru (дата обращения: 12.07.2013).

6. Бояринцев А.В., Ничиков А.В., Редькин В.Б. Общий подход к разработке моделей нарушителей // Системы безопасности. 2007. № 4.