УДК: 621.039.58
DOI: 10.30987/2658-3488-2019-2019-4-17-24

М.А.Берберова, А.С. Обоймов, А.Ю. Федорова, П.А. Росщупкина, А.А. Белая

РИСК-ИНФОРМИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ

В условиях сложной криминогенной обстановки в мире с учетом глобализации процессов мирового развития, международных политических и экономических отношений, формирующих новые риски для развития личности, общества и государства. В Российской Федерации, как и во всем мире, неуклонно возрастают угрозы безопасности промышленных объектов.

При этом в связи с повышением организованности и расширением технической оснащенности потенциальных нарушителей (террористов, экстремистов и т.д.), совершенствованием способов и методов противоправных действий особую актуальность приобретают вопросы, связанные с рационализацией технологий, направленных на защиту жизненно-важных интересов и ресурсов предприятий.

К одной из таких технологий относится создание эффективной автоматизированной системы охраны и противодействия от несанкционированного проникновения физических лиц - системы физической защиты, технически основанной на комплексе инженерно-технических средств.

Процесс проектирования комплекса инженерно-технических средств системы физической защиты промышленных объектов включает два основных этапа: концептуальное и рабочее проектирование, при этом именно от успешного проведения работ на стадии концептуального проектирования зависит оптимальность проектно-технических решений в целом.

Ключевые слова: *риск, система безопасности, система физической защиты, риск-информированная система безопасности.*

M.A. Berberova, A.S. Oboymov, A.Yu. Fedorova, P.A. Rosshchupkina, A.A. Belaya

RISK-INFORMED SECURITY SYSTEM

Under the conditions of a difficult criminal situation in the world, taking into account the globalization of world development processes, international political and economic relations, which pose new risks for the development of the individual, society and the state. In the Russian Federation, as elsewhere in the world, threats to the safety of industrial facilities are steadily increasing.

At the same time, in connection with improving the organization and expanding the technical equipment of potential violators (terrorists, extremists, etc.), improving the methods and methods of illegal actions, issues related to the rationalization of technologies aimed at protecting the vital interests and resources of enterprises are particularly relevant.

One of such technologies includes the creation of an effective automated system for the protection and counteraction against unauthorized entry of individuals - a physical protection system technically based on a set of engineering and technical means.

The design process for the complex of engineering and technical means of the physical protection system of industrial facilities includes two main stages: conceptual and detailed design, and the optimality of design and engineering solutions as a whole depends on the successful implementation of work at the conceptual design stage.

Keywords: *risk, security system, physical protection system, risk-informed safety system.*

Введение

Модель системы физической защиты (СФЗ) состоит из нескольких компонентов: модель нарушителя, модель объекта. Модель нарушителя представляет собой совокупность стратегии действий нарушителя и матриц навыков: матрицу вероятностей P(11) и матрицу времен T(12).

$$P - (p_{1.1}p_{1.2} \cdots p_{1.n}p_{2.1}p_{2.2} \cdots p_{2.n} \cdots \cdots \cdots \cdots p_{m.1}p_{m.2} \cdots p_{m.n}) \quad (1)$$

Элементом матрицы вероятностей $P_{i,j}$ является вероятность обнаружения нарушителя при преодолении элемента СФЗ *i*-го типа, используя *j*-й навык из набора навыков нарушителя.

Элементом матрицы времен $T_{i,j}$ является время преодоления элемента СФЗ *i*-го типа, используя *j*-й навык из набора навыков нарушителя.

$$T - \left(T_{1,1}T_{1,2} \cdots T_{1,n}T_{2,1}T_{2,2} \cdots T_{2,n} \cdots \cdots \cdots \cdots T_{m,1}T_{m,2} \cdots T_{m,n}\right) \quad (2)$$

В современных условиях культура физической безопасности ядерных объектов привлекает к себе повышенное внимание. Помимо других преимуществ, эффективная культура безопасности требует от персонала активных действий и инновационных подходов в условиях, когда угрозы и риски слишком многочисленны, чтобы их все могли предсказать даже самые дальновидные лидеры [1, 2].

В 2007 году общественность США была шокирована известием, что несколько профессиональных охранников были обнаружены спящими на своих постах при несении службы по охране АЭС Peach Bottom [2, 3]. Приблизительно в это же время четверо вооруженных злоумышленников ворвались на ядерную установку Pelindaba в ЮАР, где хранились сотни килограммов оружейного урана. Преступникам удалось отключить несколько уровней физической защиты объекта, однако они не были обнаружены охраной, потому что никто не следил за камерами наблюдения. После распада Советского Союза сотни радиоактивных источников, представляющих серьезную опасность для населения и содержащих радиоизотопы, которые могут быть использованы для создания «грязных» бомб, были брошены на территории ряда новообразовавшихся государств. Такие источники, наносящие вред здоровью людей и состоянию окружающее среды, до сих пор ежегодно изымаются из удаленных районов Грузии. Эти и другие, на первый взгляд случайные и не связанные между собой, инциденты имеют, тем не менее, одну общую критическую черту – «сбой» человеческого фактора.

Итальянские психологи утверждают, что из всех служащих любой фирмы 25 % - это честные люди, 25 % - ожидают удобного случая для разглашения секретов, и 50 % будут действовать в зависимости от обстоятельств [2, 4].

В 1994 году трое репортеров лондонской газеты «Санди Таймс» провели эксперимент. Представляясь бизнесменами, они вышли на двадцать депутатов британского парламента с предложением направить в правительство запрос, в котором они заинтересованы и получить за это наличными или чеком тысячу фунтов стерлингов. Из двадцати 27 сразу отказались, трое согласились. Аналогичные эксперименты проводила ФБР в начале 80-х гг.: агенты ФБР под видом арабских шейхов обращались к членам американского конгресса, предлагая им вознаграждение в десятки тысяч долларов за то, чтобы «шейхам» были устроены всякие поблажки [2, 4].

Отсюда следует вывод, что вероятность «отказа» охраны или диспетчера на пульте в результате подкупа достаточно высока. А ведь возможны еще и сценарии с ликвидации охраны КПП в результате боевого столкновения или ошибки диспетчера.

Не меньшей проблемой является предсказание действий людей в экстремальной ситуации, подобной нападению на объект нарушителей. Даже несмотря на скрупулезно разработанные инструкции и естественную логику поведения, человек в экстремальных условиях довольно часто ведет себя абсолютно непредсказуемо, иногда вообще сводя к нулю эффективность всей системы [1, 2].

Нарушение инструкции порой обходится гораздо дороже выхода из строя дорогостоящей видеокамеры или компьютера. По статистике, крупнейшие пожары начинаются с возгорания, на которое не реагируют дежурные смены специалистов. Большинство ограблений инкассаторов происходит при нарушении ими несложных служебных инструкций. Охраняемые офисы, рестораны, магазины «сдают» преступникам психологически неподготовленные охранники. Больше половины конфиденциальной

информации распространяют свои же сотрудники, подталкиваемые личной неудовлетворенностью и несложными уловками заинтересованных лиц. Таких примеров можно привести ещё много. А если речь идет об объектах повышенного техногенного риска, а в особенности, объектов ядерной энергетики, то вопрос надежности персонала вообще и персонала физической защиты в частности становится критическим.

Для задач, связанных с физическим противодействием в конфликтных ситуациях, эта проблема крайне актуальна. Предполагать отсутствие криминальных угроз охраняемым объектам невозможно, этому противоречат результаты анализа СФЗ, этому противоречит сам факт создания СФЗ. Конечно, руководитель службы безопасности уверяет руководство или владельца объекта и должен быть сам уверен, что работник охраны строго выполнит утвержденную служебную инструкцию и в условиях криминальных или террористических угроз обеспечит безопасность, не нарушая при этом законодательства и обязательств, принятых охраной. Особенно это важно при применении оружия. Тем не менее, для большинства руководителей охраны поведение охранника в той или иной нештатной ситуации остается загадкой. Так, например, зашедшие в бутик двое подростков с пневматическим пистолетом истошным криком уложили на пол здоровенного охранника, один только внешний вид которого предполагал гарантированную защиту от взвода головорезов. Покуражившиеся среди витрин подростки потребовали и получили перстень с руки охранника. В процессе разбирательства причина произошедшего так и осталось невыясненной, охранная фирма потеряла объект, уволился охранник, сменилось руководство. Однако гарантии, что столь необъяснимое явление не повторится, даются после третьей «чашки чая» и стоят недорого. И опять же, если речь идет об объектах атомной энергетики - никакого «потом» может и не быть, ни для сотрудников службы безопасности, ни для её руководства.

Не вызывает сомнения тот факт, что профессиональная готовность структур безопасности зависит от поддержания и сохранения соответствующего психологического состояния их сотрудников. Специалисты из милицейских структур утверждают, что лишь 25 % сотрудников сохраняют способность разумно действовать в экстремальных условиях; 75 % временно утрачивают ее; 10 – 12 % утрачивают ее на длительное время. По данным психологов, каждый пятый сотрудник обречен на профессиональные психологические травмы. Психологическая неподготовленность является причиной неумения собраться в экстремальных условиях (7 3%). Только около 30% сотрудников рассматриваемых структур способны самостоятельно преодолевать кризисные события, сохраняя при этом целостность личности и внутреннее равновесие, способны противостоять так называемому явлению профессиональной деформации личности [1, 2].

Люди в экстремальных условиях, характерных для охранной деятельности, часто не могут действовать грамотно, и это общая закономерность. Довольно сложно найти «идеальных мужчин», нужно уметь работать с представителями большинства homosapience, формируя из них профессионалов. Эту задачу можно эффективно решить только при организации психологической поддержки.

Однако в данной работе не вопрос психологической подготовки, а предлагается подойти к вопросу повышения уровня безопасности с другой стороны. На этапе проведения анализа эффективности СФЗ объекта, с использованием инструментов риск-информированного подхода, были описаны принципиально возможные нарушители, тактики и сценарии их действий, смоделированы как сценарии вторжения, так и сценарии контрдействий по нейтрализации нарушителя.

Задача удержания в памяти всех инструкций на все случаи действий нападающих, и, что важнее – задача своевременного обнаружения и распознания несанкционированных, враждебных действий – эти задачи очень сложны для операторов и дежурных службы безопасности любого более-менее крупного объект, этим в том числе объясняется высокая психологическая нагрузка на оператора. И эту задачу можно существенно упростить, если

обеспечить информационное сопровождение оператору, выдачей точных данных о текущем состоянии дел, помощью в обнаружении возможных нападений на ранней стадии, выдачей четких инструкций, что делать в том или ином случае.

1. Прототип риск-информированной системы безопасности

В рамках данной работы был разработан прототип риск-информированной системы безопасности, работающий по принципам, описанным выше.

В качестве основной системы, поставляющей информацию для обработки, была выбрана система видеонаблюдения. Современная видеоаналитика обладает впечатляющими возможностями, включающими распознание людей, трекинг (слежение) за людьми, в том числе и в многокамерных системах, распознание выделяющегося, подозрительного поведения, например, бег, праздношатание и многое другое [2, 5].

Однако, эти возможности во многом используются вхолостую, максимум, включая запись по обнаружению движущихся объектов и сигнализируя об этом оператору. Вся тяжесть дальнейшего анализа и принятия решений ложится исключительно на оператора. Однако, во-первых, как уже указывалось, эффективность работы оператора сильно зависит от времени суток, общей нагрузки, и многих других факторов и является недостаточной для многих случаев. А во-вторых, как показывает практика, часто операторы игнорируют происходящее на видеокамерах по привычке, например, после нескольких ложных срабатываний или после длительного периода отсутствия каких-либо попыток нарушить безопасность охраняемого объекта.

Разработанные прототип показывает принцип работы всей системы на примере одного помещения в здании.

Для демонстрации принципа работы всей системы рассматривается одно помещение – коридор. Вход в помещение охраняется сотрудником службы безопасности объекта, кроме того, вход помещение блокируется замком, например кодовым. В помещении предполагается наличие некой «запретной» зоны, в которой находится какой-либо предмет физической защиты – цель нарушителя. Камера отслеживает происходящее в помещении в автоматическом режиме, без участия оператора. Данные с видеокамеры обрабатываются программой. В случае появления кого-либо в помещении, программа начинает трекинг обнаруженных людей, отслеживая все их действия и перемещения, одновременно анализируя их.

Для помещения построены дерево событий и дерево отказов, соответствующие проникновению нарушителя в запретную зону. Заданы начальные вероятности событий и отказов. Вероятности возможных итоговых событий и отказов вычисляются в соответствии с логическими операциями, гейтам дерева.

Если обнаруживается какое-либо из событий, внесенное в дерево событий, программа автоматически отмечает событие как произошедшее (его вероятность становится равной единице), пересчитывает всё дерево и сигнализирует о повышении уровня риска (а значит, и повышение уровня угрозы безопасности), если таковое обнаруживается. Все обнаруженные события, а также соответствующие им отказы регистрируются в системе, что позволит впоследствии, при необходимости, проследить развитие событий, проанализировать действия нарушителя и персонала СФЗ, выработать предложения по улучшению СФЗ и повышению эффективности.

Дерево событий в данной программе отображает следующие ключевые события:

- Наличие движения (рис. 1). Камера зафиксировала наличие движения в помещении. В первую очередь, это означает, что обнаруженный злоумышленник каким-то образом попал в помещение, а значит, произошел отказ замка на двери или отказ охранника на входе в помещение (либо охранник нейтрализован, либо он в сговоре с нарушителем).

- Движение к запретной зоне (рис. 2). Наличие движущегося к опасной зоне человека

ещё не означает автоматически, что он движется именно в сторону «запретной зоны», однако, если движение направлено именно в эту сторону – это ещё больше повышает риск.

- Проникновение в запретную зону (рис. 3). Пока потенциальный нарушитель ещё не проник в зону, есть вероятность, что он туда и не проникнет: не успеет и его задержит группа реагирования, или он вообще пройдет мимо, или вдруг развернется и уйдет, например, если поймет, что его сейчас поймают и надо уходить. Однако, если он проник в эту зону, это автоматически означает провал группы реагирования, которая не успела или не смогла по каким-либо причинам задержать злоумышленника, отказ замка или какой-либо системы контроля доступа в «запретную» зону, если такая имеется, ну а также отказ всей системы защиты, которая допустила проникновение нарушителя в запретную зону.

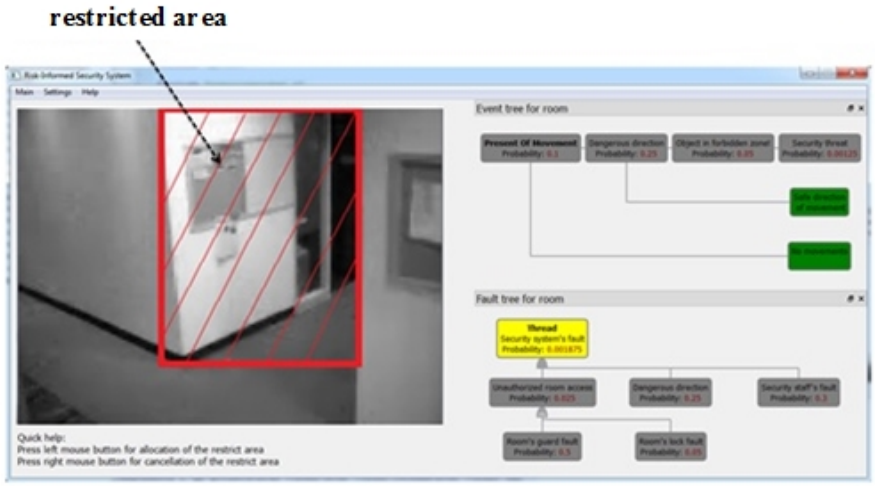

Рис. 1. Окно программы. Помещение (картинка с видеокамеры в реальном времени), «запретная» зона в помещении, дерево событий (сверху) и дерево отказов (снизу)

Рис. 2. Обнаружен нарушитель, движущийся в направлении к запретной зоне

Дерево событий выполняет функции:

- Показывает текущие распознанные события, так или иначе влияющие на уровень безопасности и риска и способные привести к негативному исходу;
- Показывает дальнейшие возможные пути и сценарии развития событий в явном виде на мониторе оператора;
- Выдает численную оценку вероятности исхода тех или иных событий.

Рис. 3. Нарушитель проник в запретную зону. Отказ СФЗ

Дерево отказов в данном случае выполняет следующие функции:

- показывает, отказ каких именно элементов привёл к тому, что нарушитель оказался в том или ином месте, преодолел тот или иной рубеж безопасности;
- показывает влияние произошедшего отказа на всю систему в целом, в явном виде показывает последствия, как возможные, так и произошедшие. Дело в том, что современные системы защиты строились на принципе единичного отказа – предполагалось, что при отказе одного из компонентов системы вся система способна обеспечить требуемый уровень защищенности. Однако, это далеко не всегда так, в сложных системах отказ одних элементов может явно или неявно влиять на работу других, повышая вероятность их отказа, а значит, и текущий уровень риска. Данная программа явно это показывает на мониторе оператора, выдавая звуковое оповещение;
- при наличии соответствующих инструкций, выдает предупреждение о необходимости включить резервные элементы СФЗ, отправить группу реагирования для проверки ситуации и, при необходимости, задержания нарушителя, предсказывает возможные отказы элементов, зависящих как-либо от уже отказавших и т.д.

Оценить масштаб вторжения можно производить по следующей методике.

Оценка масштаба вторжения характеризуется временем нахождения нарушителей в зоне контроля телекамерами, их тактикой преодоления этой зоны, временем суток, освещенностью и т.д. В зависимости от этих данных можно подбирать наиболее близкие из имеющихся в базе сценариев действий нарушителя, полученных на этапе анализа эффективности и моделирования, и предсказывать наиболее вероятные действий нарушителя, наиболее вероятные маршруты и цели, и, как следствие, быстро организовывать адекватные контрмеры.

Время нахождения нарушителя в зоне контроля телекамерой СОТ определяется как частное от деления длины контролируемой зоны на скорость движения нарушителя:

$$\tau_{пар} = \frac{2 \cdot D \cdot tg\frac{\alpha}{2}}{V_{нар}} \quad (3)$$

где:

D – расстояние от телекамеры до точки пересечения траектории нарушителя с главной оптической осью камеры (м);

α – угол обзора телекамеры (град);

$V_{нар}$ – скорость движения нарушителя (м/с).

Для телевизионных камер, контролирующих периметр объекта, принимается, что нарушителя двигается перпендикулярно главной оптической оси камеры.

Внедрение в систему модуля, моделирующего действия нарушителя, описанного в предыдущей главе. Использование данного модуля скомбинированного с методикой оценки масштаба вторжения даст оператору информацию о точном местоположении нарушителя, его количестве, а также покажет дальнейшие возможные пути нарушителя, наиболее вероятные цели, наиболее оптимальные точки для развертывания сил реагирования, а также вероятность перехвата в той или иной точке, что позволит спланировать дальнейшие действия в зависимости от обстановки.

2. Результаты

Работа с видеопотоком реализована с помощью открытой библиотеки компьютерного зрения Open CV. Программа выделяет на неподвижном фоне движущиеся объекты, и осуществляет их трекинг (слежение за объектом). Кроме того, программа работает как детектор движения, на случай, если объект как-то маскируется, и явно его выделить не получается. В этом случае, осуществляется слежение за движущимися частями.

Данный прототип показывает возможности использования системы видеонаблюдения за объектом для автоматизации работы оператора: оценка оперативной обстановки, отслеживание уровня безопасности и уровня риска, демонстрации результатов анализа в реальном времени на мониторе оператора, при наличии – вывода соответствующих инструкций и рекомендаций по дальнейшим действиям, в зависимости от обстановки.

Выводы

Дальнейшая разработка данного программного продукта и его интеграция в существующие системы физической защиты предполагает подключение к программе, как минимум, следующих функций:

- подключение к системе обработки информации с других элементов КТСФЗ: датчиков движения, инфракрасных датчиков, других сигнальных элементов.
- интеграция с системой контроля и управления доступом – в т.ч. для отслеживания действий персонала объекта и выявления внутреннего нарушителя, использующего свои полномочия для нарушения работы объекта;

Данная программа также позволяет с высокой степенью надежности (выше, чем у оператора-человека) оценивать масштаб вторжения.

Благодарность

Работа выполнена и опубликована при поддержке РФФИ, гранты 17-07-01475, 19-07-00455 и 20-07-00577.

Список литературы:

1. Обоймов, А.С. Анализ безопасности физической защиты потенциально опасных объектов / М.А. Берберова, Р.Ш. Кальметьев, Р.Т.Исламов, И.А. Кириллов, С.В. Клименко, Д.В.Минаев, А.С. Обоймов, В.П.Петров // MEDIAS-2011: труды Международной научной конференции. – Протвино-Москва: Изд. ИФТИ, 2011 - С. 114-134.

2. M.A. Berberova, A.S. Oboimov, A.Kh. Khakimova, O.V. Zolotarev, «Risk-informed security system. The use of surveillance cameras for the particularly hazardous facilities safety», Graphi Con 2019. The 29th International Conference on Computer Graphics and Vision. Conference Proceedings (2019), в печати

References:

1. Oboymov A.S. Safety Analysis of Physical Protection of Potentially Hazardous Objects / M.A. Berberova, R.Sh. Kalmetev, R.T. Islamov, I.A. Kirillov, S.V. Klimenko, D.V. Minaev, A.S. Oboimov, V.P. Petrov // MEDIAS-2011: proceedings of the International Scientific Conference.- Protvino-Moscow: Ed.ICPT, 2011 - p. 114-134.

2. M.A. Berberova, A.S. Oboimov, A.Kh. Khakimova, O.V. Zolotarev, «Risk-informed security system. The use of surveillance cameras for the particularly hazardous facilities safety», Graphi Con 2019. The 29th International Conference on Computer Graphics and Vision. Conference Proceedings (2019), in print

3. Бартош О.В., Измайлов А.В., Литвиненко Е.И., Туркин В.М. Методы и алгоритмы анализа оперативных действий сил охраны на объектах типа зданий сложной конфигурации // Специальные вопросы атомной науки и техники. Сер. Технические средства охраны. Науч.-техн. сб. - 1978. - Вып. 1 (10). - С. 60-65.
4. Андронова Е. Самое слабое звено системы безопасности. // Журнал «БДИ» №2 (53) - 2004 г.
5. Разработка рекомендаций по проведению риск-информированного анализа уязвимости и оценки эффективности систем физической защиты ядерно-опасных объектов: Отчет о НИР, рег.№ 2142ОТ11 // Международный центр ядерной безопасности - М., 2011. - 61 с.

3. Bartosh O.V., Izmailov A.V., Litvinenko E.I., Turkin V.M. Methods and algorithms for the analysis of operational actions of security forces at objects such as buildings of complex configuration // Special issues of atomic science and technology. Ser. Security equipment. Scientific and technical Sat- 1978. - Vol.1 (10).- p. 60-65.
4. Andronova E. The weakest link in the security system.// Magazine «BDI» No. 2 (53) - 2004.
5. Development of recommendations for conducting a risk-informed vulnerability analysis and evaluating the effectiveness of the physical protection systems of nuclear hazardous facilities: a research report on reg. No. 2142OT11 // International Nuclear Safety Center - M., 2011. - 61 p.

Статья поступила в редколлегию 10.10.19.
Рецензент:
к.т.н., доцент,
Брянский государственный технический университет
Подвесовский А.Г.
Статья принята к публикации 29.10.19.

Сведения об авторах:

Берберова Мария Александровна
к.т.н., научный сотрудник АНО Международный Центр по ядерной безопасности (Москва, Россия), заместитель директора по науке АНО «Научно-исследовательский Центр физико-технической информатики» (Нижний Новгород, Россия)
Тел..: +7 (916) 507-57-99
E-mail: maria.berberova@gmail.com

Обоймов Антон Сергеевич
аспирант, научный сотрудник АНО Международный Центр по ядерной безопасности (Москва, Россия)
Тел..: +7 (916) 553-78-55,
E-mail: anton.oboimov@gmail.com

Федорова Алена Юрьевна
магистрант, кафедра информационных систем в экономике и управлении АНО ВО «Российский новый университет» (Москва, Россия)
Тел..: +7 (985) 748-74-23,
E-mail: alooonka73@mail.ru

Росщупкина Полина Альбертовна
магистрант, кафедра информационных систем в экономике и управлении АНО ВО «Российский новый университет» (Москва, Россия)
Тел..: +7 (909) 623-20-47,
E-mail: kokos.polina@yandex.ru

Белая Александра Андреевна
магистрант, кафедра информационных систем в экономике и управлении АНО ВО «Российский новый университет» (Москва, Россия)
Тел..: +7 (916) 213-72-93,
E-mail: aabelaya@mail.ru

Information about authors:

Berberova Maria Aleksandrovna
Candidate of Technical Sciences, Researcher ANO International Nuclear Safety Center (Moscow, Russia), Deputy Director for Science ANO «Scientific and Research Center for Information in Physics and Technique» (Nizhny Novgorod, Russia)
Tel.: +7 (916) 507-57-99
E-mail: maria.berberova@gmail.com

Oboimov Anton Sergeevich
Graduate student, Researcher ANO International Nuclear Safety Center (Moscow, Russia)
Tel.: +7 (916) 553-78-55,
E-mail: anton.oboimov@gmail.com

Fedorova Alena Yurievna
Master student, Department of Information Systems in Economics and Management ANO HE «Russian New University» (Moscow, Russia)
Tel.: +7 (985) 748-74-23,
E-mail: alooonka73@mail.ru

Rosshchupkina Polina Albertovna
Master student, Department of Information Systems in Economics and Management ANO HE «Russian New University» (Moscow, Russia)
Tel.: +7 (909) 623-20-47,
E-mail: kokos.polina@yandex.ru

Belaya Aleksanra Andreevna
Master student, Department of Information Systems in Economics and Management ANO HE «Russian New University» (Moscow, Russia)
Tel.: +7 (916) 213-72-93,
E-mail: aabelaya@mail.ru