DOI 10.25586/RNU.V9187.18.09.P.99 УДК 004.896

**А.А. Раковенко, К.В. Быков**

# ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ ПРЕДПРИЯТИЯ В ВОПРОСАХ ФИЗИЧЕСКОГО ДОСТУПА

*В статье рассматривается совокупность различных систем, обеспечивающих безопасность предприятия, представляющего собой аппаратно-программный комплекс.*

***Ключевые слова*:** *информационная безопасность, безопасность информационных технологий, информационные системы.*

**A.A. Rakovenko, K.V. Bykov**

# ENSURING OF SECURITY OF INFORMATION OBJECTS OF THE ENTERPRISE IN MATTERS OF PHYSICAL ACCESS

*The article deals with a set of different systems that ensure the security of the enterprise, which is a hardware and software complex.*

***Keywords*:** *information security, information technology security, information systems.*

Современное состояние проблемы обеспечения безопасности предприятия определяется множеством различных факторов, важнейшими из которых являются те, которые непосредственно формируют основные оценки ситуации и принципы деятельности всех структур в сфере обеспечения безопасности предприятия. Одним из самых очевидных факторов, сформировавшихся в последнее десятилетие, является изменение характера угроз, вызванное повышением технического уровня злоумышленника, что ведет к необходимости повышения уровня автоматизации систем обеспечения безопасности предприятия (СОБП), и в частности системы физической защиты (СФЗ) как систем, непосредственно противостоящих угрозам [1; 8]. Современные СОБП включают в себя информационные объекты (ИО) как элементы системы управления, что в свою очередь требует учитывать вопрос обеспечения информационной безопасности при построении СОБП [1].

Создание системы информационной безопасности, включающей все виды средств (технические, программные и программно-технические), является чрезвычайно сложной проблемой. В частности, требуется рассматривать сильно различающиеся по принципам воздействия на ИО факторы и соответственно анализировать множество способов защиты от всех видов факторов. Поэтому целесообразно декомпозировать задачу создания системы защиты на несколько подзадач, например по видам средств защиты, и в дальнейшем объединять результаты решения в единую систему, защищающую ИО от всех видов угроз информационной безопасности.

Рассмотрим возможные угрозы негативного воздействия на ИО [2]:

1. Доступ к защищаемой информации с применением технических средств.
2. Несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам ИО;

б) использования закладочных средств;

в) использования программного обеспечения технических средств ИО через:

– маскировку под зарегистрированного пользователя;

– дефекты и уязвимости программного обеспечения ИО;

– внесение программных закладок;

– применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

– несанкционированного физического доступа к ИО;

– хищения носителя информации.

3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

4. Действия криминальных групп и отдельных преступных субъектов:

а) диверсия в отношении ИО;

б) диверсия в отношении элементов ИО.

5. Искажение, уничтожение или блокирование информации с применением технических средств путем:

а) преднамеренного силового электромагнитного воздействия:

– по сети электропитания на порты электропитания постоянного и переменного тока;

– по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

– по металлоконструкциям на порты заземления и порты корпуса;

– посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи;

б) преднамеренного силового воздействия различной физической природы;

в) использования программных или программно-аппаратных средств при осуществлении:

– компьютерной атаки;

– сетевой атаки;

г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

Объекты информатизации включают автоматизированные системы управления различными процессами. Выход из строя этих систем приводит к нарушению функционирования системы управления, что может повлечь за собой катастрофические последствия. Обеспечение информационной безопасности в системе управления предприятием достигается путем принятия в рамках системы защиты автоматизированной системы управления совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса [5; 6; 7].

Перечень этапов решения задачи обеспечения информационной безопасности предприятия [3]:

1) сбор и обработка экспертной информации о характеристиках угроз;

2) сбор и обработка экспертной информации для определения важности выполнения требований для устранения различных угроз;

3) оценка стоимости системы защиты информации для конкретного варианта ее реализации;

4) разработка математической модели и алгоритма выбора рационального варианта построения системы защиты информации.

Технические средства защиты как часть общей системы информационной безопасности в совокупности представляют собой СФЗ. От эффективности СФЗ зависит возможный информационный, экономический и материальный ущерб, и в крайних

случаях, нарушение информационной безопасности приводит к возникновению катастрофы на высокотехнологичном производстве предприятия. СФЗ представляют собой объединение сил охраны и технического оснащения – комплекса инженерно-технических средств охраны (рис. 1).

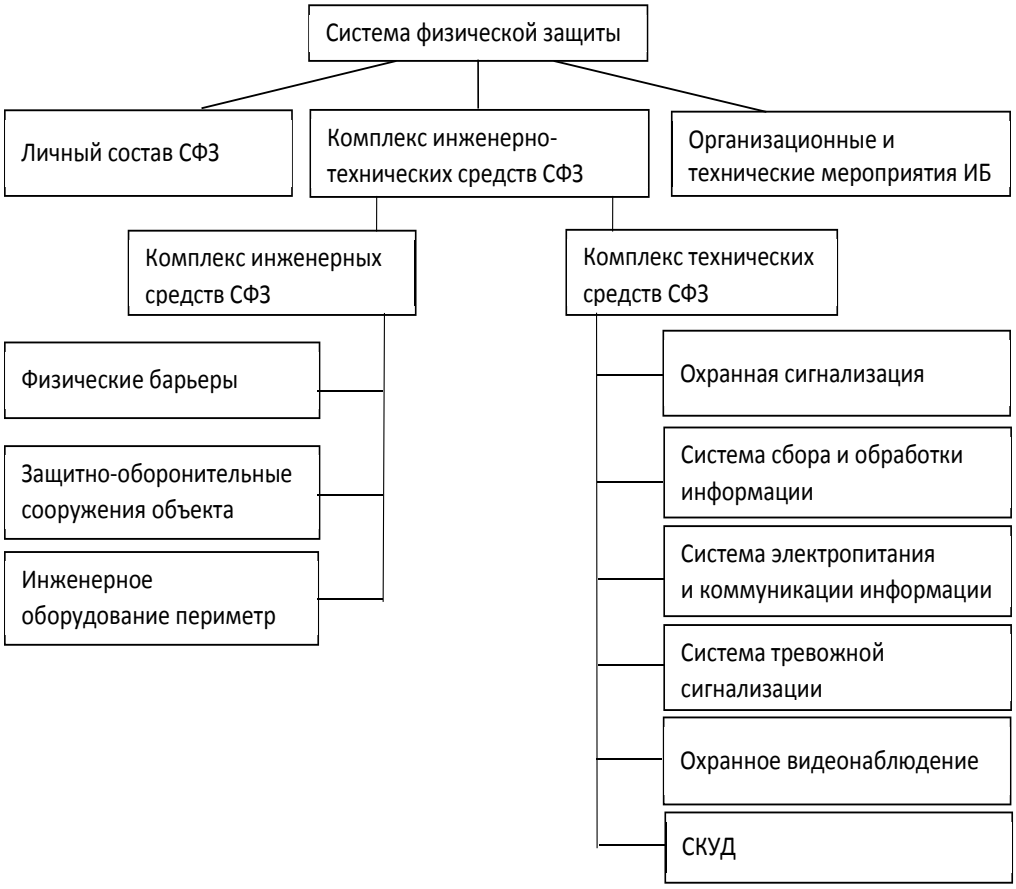


**Рис. 1.** Обобщенная структурная схема системы физической защиты

Создание СФЗ – это сложный процесс, если при создании будут допущены ошибки или не будут учтены все факторы и условия, то полученная система либо не сможет противодействовать угрозам, либо превысит необходимый уровень защищенности для ИО и затраты на ее создание и обслуживание будут необоснованно высоки. Поэтому физическая безопасность ИО напрямую зависит от результатов решения задачи создания СФЗ. Особое внимание стоит уделить автоматизированной системе охраны (АСО), с помощью которой реализуются практические меры по предупреждению несанкционированного доступа к аппаратуре, оборудованию, материалам, документам и охране их от шпионажа, диверсий, повреждений, хищений и других незаконных или преступных действий. На практике действия АСО складываются из двух основных фаз: обнаружение нарушителя (в возможно короткий период времени с момента его появления в охраняемой зоне) и его задержание. Задачи обнаружения нарушителя и определения места его проникновения могут быть решены как с помощью патрулей

из личного состава службы охраны, так и с помощью технических средств охраны. Задачи обнаружения нарушителя и контроля за состоянием безопасности охраняемых предприятий решаются главным образом с помощью технических средств охраны и телевизионного наблюдения. Применение этих средств позволяет в разумных пределах (с точки зрения реализации определенной тактики охраны) снизить численность личного состава охраны, но при этом повысить надежность защиты предприятия, увеличить оперативность в принятии мер к задержанию нарушителя [4].

При проектировании СФЗ используется исходная информация, отражающая опыт и знания экспертов. Знания экспертов обычно являются результатами приблизительных оценок, прогнозов и предположений. При этом не стоит забывать, что при создании СФЗ предприятия необходимо учитывать условия функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и обстановки и т. д. Таким образом, для каждого конкретного предприятия должна разрабатываться на основе общей своя собственная СОБП, исходя из положений которой разрабатывается проект оснащения предприятия инженерно-техническими, специальными и программно-аппаратными средствами защиты. Необходимо выделить этапы процесса проектирования СФЗ ИО с целью формулировки и конкретизации подзадач, соответствующих этапам решения общей задачи создания, определить этапы, которые реализуются с использованием средства информационных технологий, использовать уже имеющиеся способы решения подзадач, а также определить этапы, для которых в настоящее время уже существует информационная поддержка [4].

На основе вышесказанного можно определить критически важные подзадачи для создания СФЗ предприятия:

– характеристика системы охраны: сбор и анализ информации об объекте (анализ организации существующей системы охраны предприятия: реагирование сил охраны на сигналы тревоги, на сигналы в случае аварии на предприятии, комплексная проверка системы охраны; план территории предприятия, схема объекта, чертежи коммуникационных систем, размещение существующих средств охраны и т. д.);

– формирование списка угроз: определение категорий нарушителей, определение потенциальных целей нарушителей и их приоритетность, возможная тактика их действия, их технические возможности и опыт, количественные характеристики угроз: вероятность угрозы, значимость угрозы, время до ближайшей угрозы и т. д.;

– выявление целей нападения: имущество, информация, люди и т. п., возможные потери в случае диверсии. На основе анализа проводится категорирование всего предприятия (цеха, производства и т. д.), выделение отдельных зон и помещений, разделение их по категориям ущерба, определение для каждой зоны нормативных показателей уязвимости и т. д.

Среди этапов можно выделить подготовительные: сбор и систематизация исходных данных, этапы обработки полученной информации. Если сбор информации является работой экспертов, которую нельзя заменить работой средств вычислительной техники, то процессы обработки информации являются как раз теми этапами проектирования СФЗ ИО, для которых можно реализовать информационную поддержку. Необходимо также определить, какие этапы могут проводиться с использованием информационной поддержки для помощи экспертам в решении задачи проектирования.

Для реализации этих этапов необходимо описать методы, программная реализация которых будет представлять собой информационную поддержку решения задачи каждого этапа, сформулировать требования к методам и приблизительный состав алгоритмов.

1. Определение требований к системе физической защиты ИО. Метод определения требований должен объединять в себе обработку всех исходных данных о предприятии (экспертную информацию), и результатом его работы будут оценки текущей

защищенности и требуемой защищенности. Оценка требуемой защищенности будет использована для дальнейшего создания концептуального проекта СФЗ. Информация о требуемых уровнях защищенности критических элементов объекта должна быть достаточной для определения характеристик средств защиты каждого критически важного элемента (КВЭ) с необходимой степенью детализации. Информация о требуемой защищенности также должна быть формализована, чтобы ее можно было использовать в качестве исходных данных для последующих алгоритмов.

2. Создание проекта СФЗ ИО. Метод создания концептуального проекта системы защиты требует формализации СФЗ, т. е. описания будущей СФЗ в виде модели. Модель СФЗ должна соответствовать модели объекта и форме представления исходных данных о требуемой защищенности. Метод должен включать в себя алгоритмы, результатов работы которых достаточно для получения информации о необходимом составе СФЗ на предприятии, причем с обязательным указанием, на каком участке объекта должен быть установлен каждый элемент СФЗ [9].

3. Оценка проекта системы физической защиты ИО. Метод оценки нужен для определения достаточности защиты предприятия, т. е. для анализа качества проекта СФЗ. Результатом оценки будет вывод о пригодности проекта для создания системы защиты на реальном объекте. Метод частично повторяет первый, и в нем могут использоваться похожие алгоритмы:

– оценка текущего уровня защищенности объекта и его КВЭ;

– оценка соответствия уровня защищенности объекта и его КВЭ требуемым уровням защищенности.

Таким образом, безопасность предприятия обеспечивается совокупностью различных систем, основной из которых является система физической защиты. При построении требуемой системы физической защиты на различных этапах проектирования создания должны быть сформулированы требования к методам и приблизительный состав алгоритмов с учетом уже имеющихся методов поддержки принятия решения. Системы безопасности предприятия на сегодняшний день представляют собой аппаратно-программные комплексы с общей базой данных, интегрированные в общую систему управления предприятием. В качестве устройств управления используются компьютерные терминалы со специализированным программным обеспечением. В связи с этим при проектировании таких систем необходимо выделить отдельным направлением создание системы для обеспечения безопасности имеющихся ИО предприятия как аппаратно-программного комплекса, учитывая возможность интегрирования его в единую систему обеспечения защиты предприятия.

**Литература**

1. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. № Пр-646. – М., 2016. – 16 с.

2. ГОСТ Р 51275–2006. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М., 2007. – 7 с.

3. *Родичев Ю.А.* Нормативная база и стандарты в области информационной безопасности : учеб. пособие / Ю.А. Родичев. – СПб. : Питер, 2017. – 256 с.

4. *Семененко В.А.* Информационная безопасность : учеб. пособие. – 4-е изд., стер. / В.А. Семененко. – М. : МГИУ, 2010. – 277 с.

5. Лозовецкий В.В. Информационная безопасность : учеб. пособие / В.В. Лозовецкий. – М. : ИУИИ, 2011. – 168 с.

6. *Бирюков А.А.* Информационная безопасность: защита и нападение / А.А. Бирюков. – М. : ДМК Пресс, 2012. – 474 с.

7. *Домарев В.В.* Безопасность информационных технологий. Системный подход / В.В. Домарев. – К. : ТИД Диа Софт, 2004. – 992 с.

8. *Гладышев А.И., Аборкина Е.С.* Вопросы применения существующих методов оценки сложности информационных систем // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ, управление. – 2016. – Вып. 1–2. – С. 114–118.

9. *Гладышев А.И.* Вопросы математического моделирования радиоинформационных систем // Вестник Российского нового университета. Сер. Сложные системы: модели, анализ, управление. – 2016. – Вып. 1–2. – С. 46–52.

**References**

1. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № Pr-646. – M., 2016. – 16 s.

2. GOST R 51275–2006. Ob”ekt informatizatsii. Faktory, vozdeystvuyushchie na informatsiyu. Obshchie polozheniya. – M., 2007. – 7 s.

3. *Rodichev, Yu.A.* Normativnaya baza i standarty v oblasti informatsionnoy bezopasnosti : uchebnoe posobie / Yu.A. Rodichev. – SPb. : Piter, 2017. – 256 s.

4. *Semenenko, V.A.* Informatsionnaya bezopasnost’ : ucheb. posobie. – 4-e izd., ster. / V.A. Semenenko. – M. : MGIU, 2010. – 277 s.

5. *Lozovetskiy, V.V.* Informatsionnaya bezopasnost’ : ucheb. posobie / V.V. Lozovetskiy. – M. : IUII, 2011. – 168 s.

6. *Biryukov, A.A.* Informatsionnaya bezopasnost’: zashchita i napadenie / A.A. Biryukov. – M. : DMK Press, 2012. – 474 s.

7. *Domarev, V.V.* Bezopasnost’ informatsionnykh tekhnologiy. Sistemnyy podkhod / V.V. Domarev. – K. : TID Dia Soft, 2004. – 992 s.

8. *Gladyshev, A.I., Aborkina, E.S.* Voprosy primeneniya sushchestvuyushchikh metodov otsenki slozhnosti informatsionnykh sistem // Vestnik Rossiyskogo novogo universiteta. Ser. Slozhnye sistemy: modeli, analiz, upravlenie. – 2016. – Vyp. 1–2. – S. 114–118.

9. *Gladyshev, A.I.* Voprosy matematicheskogo modelirovaniya radioinformatsionnykh sistem // Vestnik Rossiyskogo novogo universiteta. Ser. Slozhnye sistemy: modeli, analiz, upravlenie. – 2016. – Vyp. 1–2. – S. 46–52.