УДК 004.896 DOI: 10.18698/2541-8009-2023-11-953

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ДЛЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Н.В. Ядыкин yadyykinnv@student.bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрены общие принципы инженерно-технической защиты информации, а также ее иерархическая структура. Большое внимание уделено актуальной на сегодняшний день теме — применению интеллектуальных систем для организации инженерно-технической защиты информации. Исследована роль интеллектуальных систем в организации защиты, представлены перспективы их подобного использования. Кроме того, рассмотрена возможность применения интегрированных систем, обладающих единым программным обеспечением, которое дает возможность соединять все потоки поступающих данных, создавая при этом общую компьютерную систему управления и контроля, которая обеспечивает безопасность объекта.

Ключевые слова

Защита информации, безопасность, интеллектуальные системы, инженерно-техническая защита информации, технические системы безопасности, система охранной сигнализации, системы пожарной сигнализации, системы видеонаблюдения, системы контроля и управления доступом, технические средства охраны, интегрированная техническая система охраны

Поступила в редакцию 19.10.2023

Введение. Инженерно-техническая защита информации объективно приобретает все больший вес. Такая тенденция обусловлена следующими причинами:

– развитием методов и средств добывания информации, позволяющих несанкционированно получать все больший объем информации на безопасном расстоянии от ее источников;

– огромными достижениями микроэлектроники, способствующими созданию технической базы для массового изготовления доступных рядовому покупателю средств нелегального добывания информации. Доступность миниатюрных и камуфлированных технических средств добывания информации превращает задачу нелегального добывания информации из уникальной и рискованной операции в прибыльный бизнес, что увеличивает число любителей добиваться легкой наживы противозаконными действиями;

– оснащением служебных и жилых помещений, а также в последнее время автомобилей, разнообразной электроаппаратурой и радиоэлектронной аппаратурой, физические процессы в которой способствуют случайной неконтролируемой передаче (утечке) конфиденциальной информации из помещений и автомобилей.

Очевидно, что эффективная защита информации с учетом этих тенденций возможна при более широком использовании технических средств защиты

с применением интеллектуальных интегрированных технических систем безопасности.

Принципы инженерно-технической защиты информации. Технология защиты информации, как и любая другая, должна отвечать определенным общепринятым требованиям, которые можно рассматривать как общие принципы защиты информации. К ним относятся:

– надежность и непрерывность;
– скрытность и целеустремленность;
– рациональность;
– активность;
– гибкость;
– многообразие способов;
– комплексное использование различных способов и средств;
– экономичность [1].

В общих принципах инженерно-технической защиты информации не содержится конкретных рекомендаций по организации защиты. Однако они ориентируют специалиста на требования, которым должна соответствовать инженерно-техническая защита информации [2].

Структура системы инженерно-технической защиты информации. Система инженерно-технической защиты информации имеет иерархическую структуру. Ее первый уровень образуют подсистемы, следующий уровень — комплексы, затем — подкомплексы. Каждый структурный элемент объединяет силы и средства, позволяющие решать определенные задачи системы. В состав системы инженерно-технической защиты информации входят подсистемы физической защиты информации и защиты ее от утечки (см. рисунок).

Структура системы инженерно-технической защиты информации

Подсистема физической защиты источников информации отвечает за предотвращение проникновения к источникам защищаемой информации злоумышленников и стихийных сил природы, прежде всего пожара. Основными ее составляющими служат комплексы инженерной защиты источников информации и их технической охраны [3].

Подсистема защиты информации от утечки предназначена для того, чтобы выявлять технические каналы утечки информации, а также противодействовать утечке информации по этим каналам. Каналы утечки могут быть обнаружены по их демаскирующим признакам. Но проблемой является то, что технические датчики трудно обнаруживают признаки носителей информации в канале утечки, поэтому каналы в основном обнаруживаются по косвенным признакам. Поскольку косвенные признаки обычно недостаточно информативны, выявить с помощью них каналы утечки могут только специалисты с высоким уровнем подготовки [4].

Неопределенность видов и времени проявления угроз информации, большое количество и разнообразие средств ее защиты, дефицит времени в случаях чрезвычайных ситуаций предъявляют повышенные требования к управлению элементами системы инженерно-технической защиты информации. Элементы управления образуют комплекс управления. Он должен обеспечить:

– реализацию общих принципов защиты информации;

– согласование в рамках единой системы функционирования подсистемы физической защиты информации и подсистемы защиты ее от утечки;

– оперативное принятие решений по защите информации;

– контроль эффективности мер защиты.

Комплекс управления позволяет согласовывать деятельность сил и средств защиты подсистем физической защиты и защиты от утечки, поскольку данные подсистемы обычно курируются разными ведомствами, а пользователь информации один [5].

Интеллектуализация инженерно-технической защиты информации. Интеллектуализация — одна из основных современных тенденций развития информационных систем, и сфера инженерно-технической безопасности не стала исключением. Технологии интеллектуализации применяют в задачах обнаружения различного рода угроз безопасности, выявления аномалий, корреляции событий при анализе инцидентов безопасности, поддержки принятия решений при формировании оптимальной конфигурации системы защиты информации и выборе средств защиты [6]. Все это стало возможно благодаря современным интеллектуальным комплексам, которые обладают разнообразной элементной базой, инновационными подходами к проектированию и внедрению оборудования. Большинство из этих комплексов являются интегрированными системами и обладают единым программным обеспечением (ПО). Единое ПО дает возможность объединять все потоки данных, создает при этом общую компьютерную систему управления и контроля, которая обеспечивает безопасность.

Достичь необходимого уровня безопасности объекта защищаемой информации можно разными способами. Для охраны обычно применяют стандартные технические системы безопасности (ТСБ), такие как:

– система охранной сигнализации (включая защиту периметра объекта и тревожное оповещение) (СОС);

– системы пожарной сигнализации (включая аварийное оповещение и управление эвакуацией персонала и посетителей) (СПС);

– системы видеонаблюдения (СВК);

– системы контроля и управления доступом (СКУД);

Отметим, что обширная интеграция ТСБ возможна только в том случае, если на объекте поддерживаются основные, базовые уровни интеграции, основанные на организационно-административных способах защиты объектов и средствах и методах инженерно-технической защиты.

Наиболее эффективное решение при установке технических средств охраны (ТСО) заключается в использовании принципов системного интегрирования и создании многофункционального технического комплекса, совмещающего в себе функции всех традиционных автономных систем.

Интегрированная техническая система охраны (ИТСО) предусматривает объединение на базе современных информационных технологий и программно-аппаратной интеграции нескольких подсистем, которые функционально и информационно связаны между собой, имеют одно ПО, позволяющее объединить все потоки поступления данных и создать одну компьютерную систему управления объектом и его контроля, обеспечивающую безопасность. Даже с минимальным уровнем интеграции взаимодействие подсистем осуществляется так, что события одной подсистемы влияют на другую и вызывают определенные реакции. ИТСО, созданная на базе традиционных подсистем СОС, СКУД, СВК и СПС, обеспечивает, к примеру, следующее взаимодействие между подсистемами:

– при поступлении сигнала пожарной тревоги (от СПС) разблокирует двери и проходы (СКУД), используемые при эвакуации, в зонах возможного пожара или по всему объекту;

– при срабатывании различных охранных детекторов (в СОС) или детекторов активности от видеокамер (в СВК) блокирует охраняемые зоны, тамбуры, шлюзы (СКУД);

– при поступлении тревожных сигналов (от СПС, СКУД и СОС) подключает соответствующие видеокамеры (СВК), с помощью которых уточняется и документируется обстановка в зоне тревоги [7].

Использование интегрированных систем безопасности по сравнению с использованием отдельных систем и средств защиты обеспечивает такие преимущества, как:

– более быстрая и точная реакция на происходящие события;

– более оптимальный анализ текущей ситуации;

– снижение риска «человеческого фактора» за счет уменьшения ошибок и возможных недобросовестных действий обслуживающего персонала и сотрудников организации;

– уменьшение расходов на оборудование благодаря многофункциональному использованию отдельных ТС и более полной их загрузке;

– упрощение работы обслуживающего персонала в результате того, что процессы управления, контроля и принятия решений по обеспечению безопасности автоматизированы;

– снижение затрат на содержание и обучение обслуживающего персонала, а также на монтаж и эксплуатацию системы безопасности [8].

Как правило, технические системы безопасности строятся по централизованному принципу, на центральном посту охраны размещается основная аппаратура управления и контроля, позволяющая принимать наиболее рациональные и оперативные решения при возникновении нештатных ситуаций. Однако, как показала практика, чрезмерная централизация снижает живучесть и надежность систем безопасности. Для того чтобы улучшить эти характеристики, в ИТСО желательно частично перенести оборудование центрального поста охраны на пространственно-удаленное резервное рабочее место. Данные, полученные от ИТСО, также могут использоваться на рабочем месте администратора ЛВС, оператора бюро пропусков, сотрудника отдела кадров, диспетчера систем инженерного обеспечения, сотрудника службы безопасности компании. При этом для ИТСО со средним уровнем интеграции желательно сохранить некоторую автономность для каждой подсистемы — это будет обеспечивать безопасность всей системы в случае, если одна из подсистем выйдет из строя, а также повысит общую надежность работы ИТСО.

Отметим, что ИТСО нельзя строить как полностью автоматизированную систему, поскольку невозможно формализовать все реально встречающиеся ситуации на конкретном объекте. Поэтому прежде всего нужно автоматизировать стандартный рутинный процесс работы, но окончательное решение о наиболее важных аспектах безопасности объекта должен принимать все-таки человек.

Основное назначение интегрированной системы заключается в том, чтобы обеспечить оператору системы максимально удобный и легкий контроль ситуации на объекте и предоставить ему четкую обработанную информацию, которая не требует никаких действий в стрессовой ситуации. Базовой архитектурой ИТСО является центральный компьютер с терминалом оператора и принтером, подключаемый к контроллеру той или иной подсистемы.

Компьютер подключают к информационно-телекоммуникационной сети организации ИТСО, например, к локальной вычислительной сети (ЛВС). Тем самым обеспечивается многопользовательский режим работы с ИТСО и управление техническими средствами интегрированных систем по стандартным цифровым протоколам, совместимым с интерфейсами ЛВС.

В ИТСО компьютер предпочтительнее устанавливать по типу сервера, это обеспечит его надежную и круглосуточную работу. В связи с этим предъявляют особые требования к используемым в компьютере комплектующим изделиям и техническим решениям, в том числе к интеллектуальной системе бесперебойного питания и энергосбережения, горячему резервированию, контролю внутренней температуры системного блока.

Системой более высокого уровня в сравнении с ИТСО является интегрированная техническая система безопасности (ИТСБ), которая объединяет все инженерно-технические системы объекта.

Наряду с ИТСО ИТСБ может охватывать следующие системы:

– информационно-аналитическую, обеспечивающую анализ рисков, возможных угроз, юридической защиты;

– экономической безопасности, реализующую защиту от недобросовестной конкуренции, возврат кредитов, проверку клиентов;

– собственной безопасности, обеспечивающую проверку сотрудников на лояльность, досмотр посетителей, персонала и корреспонденции, экологический мониторинг, контроль систем жизнеобеспечения объекта;

– защиты информации в информационно-вычислительных и телекоммуникационных сетях;

– защиты информации от утечки по техническим каналам;

– автоматического пожаротушения и дымоудаления;

– физической охраны объекта;

– обеспечения безопасности автоперевозок [9].

На базе инновационных информационных технологий интегрируются не только ТСБ, но также вычислительные системы, системы инженерного обеспечения здания, телекоммуникационные системы, тем самым создается концепция «интеллектуального здания» [10].

Заключение. Хотелось бы еще раз обратить внимание на то, что современная и надежная инженерно-техническая защита информации не может быть эффективной без внедрения интеллектуальных систем. С ростом автоматизации управления во всех сферах жизнедеятельности, созданием специализированных автоматизированных систем для управления целыми отраслями промышленности, субъектами федерации, военными округами критичность сохранения конфиденциальности, целостности и доступности информации, обрабатываемой в подобных автоматизированных системах, очень велика. Ущерб от нарушения информационной безопасности может исчисляться сотнями миллионов рублей и приводить к необратимым последствиям, оказывая влияние на жизнеспособность государства в целом.

Что касается многих других вопросов инженерно-технической защиты информации (подробное описание путей построения подсистем ИТСО, маркетинговая проработка существующих технических средств и систем обеспечения безопасности), то эти актуальные темы достойны рассмотрения в отдельных статьях.

Литература

[1] Торокин А.А. *Инженерно-техническая защита информации*. Москва, Гелиос АРВ, 2005, 934 с.

[2] *Методы, способы и средства инженерно-технической защиты информации*. URL: https://studfile.net/preview/3619184/page:20/ (дата обращения 14.05.2023).

[3] Хорев А.А. *Технические каналы утечки акустической (речевой) информации*. Москва, Аналитика, 1998, 436 с.

[4] Каторин Ю.Ф., Разумовский А.В., Спивак А.И. *Защита информации техническими средствами*. Санкт-Петербург, НИУ ИТМО, 2012, 416 с.

[5] *Структура системы инженерно-технической защиты информации*. URL: https://studopedia.ru/18_70411_struktura-sistemi-inzhenerno-tehnicheskoy-zashchiti-informatsii.html (дата обращения 14.05.2023).

[6] Васильева И.Н. *Интеллектуальные системы защиты информации*. Санкт-Петербург, СПбГЭУ, 2020, 119 с.

[7] *Технические основы охраны фирмы*. URL: http://www.r-control.ru/articles/safetysystem/article4 (дата обращения 14.05.2023).

[8] *Система Интеллект: основные преимущества и составляющие элементы оборудования*. URL: https://camafon.ru/sistemyi-bezopasnosti/intellektualnyie (дата обращения 14.05.2023).

[9] *Системы безопасности.* URL: https://camafon.ru/sistemyi-bezopasnosti/intellektualnyie (дата обращения 14.05.2023).

[10] *Организационное обеспечение физической защиты объекта информации*. URL: https://en.ppt-online.org/724694 (дата обращения 14.05.2023).

Ядыкин Никита Владимирович — студент кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Миков Дмитрий Александрович, доцент кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация. E-mail: mikovda@yandex.ru; SPIN-код: 1879-2274.

Ссылку на эту статью просим оформлять следующим образом:
Ядыкин Н.В. Интеллектуальные системы в инженерно-технической защите информации. *Политехнический молодежный журнал*, 2023, № 11 (88).
http://dx.doi.org/10.18698/2541-8009-2023-11-953

INTELLIGENT SYSTEMS IN THE INFORMATION ENGINEERING AND TECHNICAL PROTECTION

N.V. Yadykin yadyykinnv@student.bmstu.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper considers general principles of the information engineering and technical protection, as well as its hierarchical structure. Significant attention is paid to the topic that is relevant today, i.e. using the intelligent systems in organizing the information engineering and technical protection. The role of intelligent systems in organizing protection is analyzed, and the prospects for its similar use are presented. In addition, possibility of using integrated systems with the unified software is considered making it possible to connect all the incoming data streams and to create a common computer management and control system that ensures the object safety and security.

Keywords

Information protection, security, intelligent systems, information engineering and technical protection, technical security systems, security alarm system, fire alarm systems, video surveillance systems, access control and management systems, technical security equipment, integrated technical security system

Received 19.10.2023

References

[1] Torokin A.A. *Inzhenerno-tekhnicheskaya zashchita informatsii* [Engineering and technical information protection]. Moscow, Gelios ARV Publ., 2005, 934 p. (In Russ.).

[2] *Metody, sposoby i sredstva inzhenerno-tekhnicheskoy zashchity informatsii* [Methods and means of engineering and technical information protection]. URL: https://studfile.net/preview/3619184/page:20/ (accessed May 14, 2023).

[3] Khorev A.A. *Tekhnicheskie kanaly utechki akusticheskoy (rechevoy) informatsii* [Technical channels for leaking acoustic (speech) information]. Moscow, Analitika Publ., 1998, 436 p. (In Russ.).

[4] Katorin Yu.F., Razumovskiy A.V., Spivak A.I. *Zashchita informatsii tekhnicheskimi sredstvami* [Protecting information by technical means]. Sankt-Petersburg, NIU ITMO Publ., 2012, 416 p. (In Russ.).

[5] *Struktura sistemy inzhenerno-tekhnicheskoy zashchity informatsii* [Structure of the engineering and technical information protection system]. URL: https://studopedia.ru/18_70411_struktura-sistemi-inzhenerno-tehnicheskoy-zashchiti-informatsii.html (accessed May 14, 2023).

[6] Vasil'eva I.N. *Intellektual'nye sistemy zashchity informatsii* [Intelligent information security systems]. Sankt-Petersburg, SPbGEU Publ., 2020, 119 p. (In Russ.).

[7] *Tekhnicheskie osnovy okhrany firmy* [Technical basis of company security]. URL: http://www.r-control.ru/articles/safetysystem/article4 (accessed May 14, 2023).

[8] *Sistema Intellekt: osnovnye preimushchestva i sostavlyayushchie elementy oborudovaniya* [Intellect system: main advantages and components of the equipment]. URL: https://camafon.ru/sistemyi-bezopasnosti/intellektualnyie (accessed May 14, 2023).

[9] *Sistemy bezopasnosti* [Security systems]. URL: https://camafon.ru/sistemyi-bezopasnosti/intellektualnyie (accessed May 14, 2023).
[10] *Organizatsionnoe obespechenie fizicheskoy zashchity ob"ekta informatsii* [Organizational provision of physical protection of the information object]. URL: https://en.ppt-online.org/724694 (accessed May 14, 2023).

Yadykin N.V. — Student, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Mikov D.A., Associate Professor, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation. E-mail: mikovda@yandex.ru, SPIN-code: 1879-2274.

Please cite this article in English as:
Yadykin N.V. Intelligent systems in the information engineering and technical protection. *Politekhnicheskiy molodezhnyy zhurnal*, 2023, no. 11 (88). (In Russ.).
http://dx.doi.org/10.18698/2541-8009-2023-11-953