ПРАВОВОЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

*Алексеев В.В., Емельянов Е.В., Кастерин Д.А., Стрельцов А.А.**

Ключевые слова: *информация, привилегированная информация, правовое обеспечение, информационная безопасность, угрозы, система защиты, типовая структура, нормативные документы, организационно-техническая система.*

Аннотация.

Цель работы: *исследование взаимосвязи этапов построения системы защиты информации в организации с учетом соответствующих групп нормативно-правовых документов и законодательных актов.*

Метод: *руководствуясь системным подходом, авторы попытались проследить степень влияния требований определенных нормативно-правовых документов и законодательных актов на принимаемые разработчиками решения по составу и взаимосвязям элементов системы защиты информации в организации.*

Результаты: *предложен ряд обобщенных технических решений по конфигурации элементов системы защиты информации в организации; основным результатом исследования следует считать вывод о том, что правовое обеспечение при построении системы защиты информации организационно-технической системы имеет важное значение и предварительный учет требований нормативно-правовых документов по обеспечению защиты информации позволяет более точно определить ее структуру и параметры.*

DOI: 10.21681/1994-1404-2020-2-54-61

Введение

Сегодня активно развивается такой класс сложных систем, как организационно-технические системы (ОТС). Естественно, что большое количество разработчиков аппаратно-программного обеспечения создает технологии и инструменты, призванные защитить привилегированную[1] информацию, формируемую в системе, от «нежелательных глаз» [10]. При этом многие разработчики часто забывают о том, что процессы защиты информации в системе достаточно жестко регулируются законодательством Российской Федерации и нормативно-правовыми документами соответствующих федеральных органов и учреждений [12].

При функционировании ОТС генерируется *конфиденциальная* информация, поэтому возникает необходимость организовать соответствующую систему защиты информации. Этапы построения системы защиты информации в организации, как правило, коррелируют с этапами построения модели системы. Защита информации в организации должна быть разработана с использованием норм и требований руководящих документов и законов Российской Федерации в области защиты информации[2]. В организации обязательно

[1] *Например,* научно-техническую, финансово-экономическую, производственную, организационно-технологическую, конъюнктурную, патентно-лицензионную и др. информацию, обладающую ценностью (в материальном, моральном и ином аспекте) в силу неизвестности ее третьим лицам.

[2] *См., в частности:* Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ; Федеральный закон РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ; Федеральный закон РФ «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ; Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 9 сентября 2000 г. № Пр-1895; Приказ ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 г. № 17; Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21; РД. Автоматизированные системы. Защита от несанкцио-

** **Алексеев Владимир Витальевич,** доктор технических наук, профессор, член-корреспондент РАЕН, почетный радист РФ, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, Российская Федерация, г. Тамбов.*

E-mail: *vvalex1961@mail.ru*

Емельянов *Евгений Валентинович, аспирант Федерального центра науки и высоких технологий «СНПО «Элерон», Российская Федерация, г. Москва.*

E-mail: *evemelyanov@rosatom.ru*

Кастерин *Дмитрий Александрович, оператор научной роты Межвидового центра подготовки и боевого применения войск радиоэлектронной борьбы, Российская Федерация, г. Тамбов.*

E-mail: *dmitkast1996@mail.ru*

Стрельцов *Алексей Андреевич, аспирант Федерального центра науки и высоких технологий «СНПО «Элерон», Российская Федерация, г. Москва.*

E-mail: *alastreltsov@rosatom.ru*

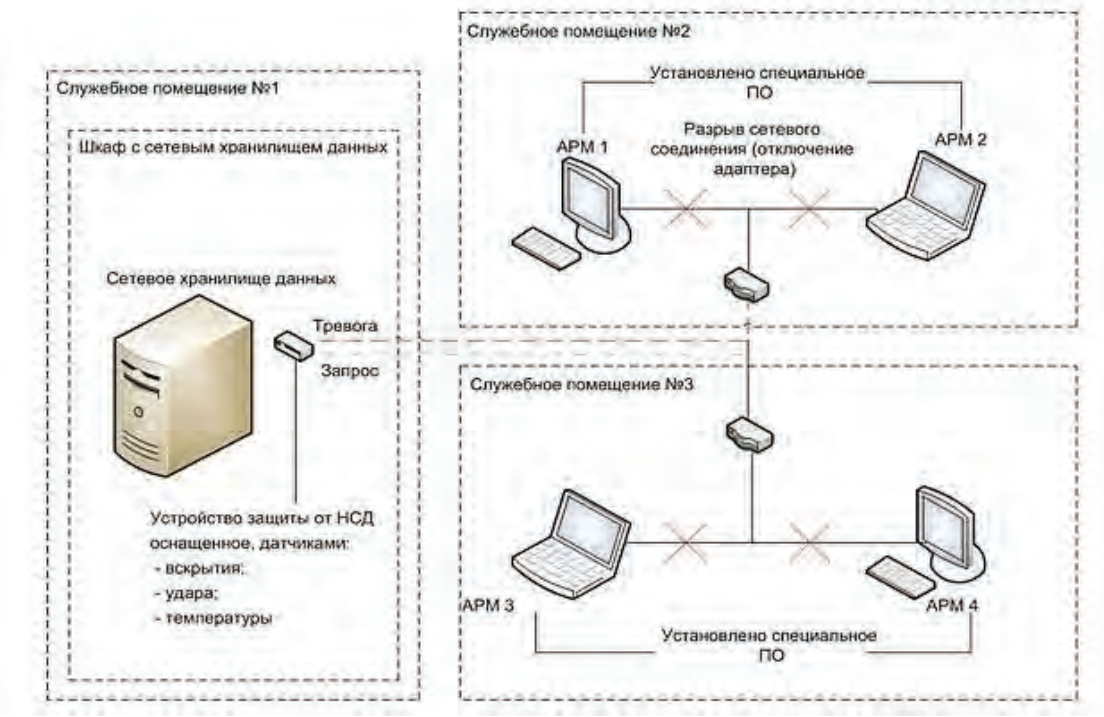

Рис. 1. Типовая структура подсистемы защиты от несанкционированного доступа

наличие следующих основных нормативных документов и локальных актов в области защиты информации:

- «Руководство по защите конфиденциальной информации»;
- «Устав организации»;
- «Положение о подразделениях»;
- «Положение о порядке организации и проведению работ по защите информации»;
- «Руководство по контролю за состоянием системы защиты информации»;
- «Руководство о системах технической защиты информации».

В зависимости от предназначения и стратегии развития ОТС, в ней применяют как отдельные элементы организационной, программной или аппаратной системы защиты информации, так и их сочетание [1]. В связи с этим целесообразно обосновать *типовые структуры* подсистем защиты информации в ОТС, интегрируемые в соответствующую систему, характеристики которой будут удовлетворять требованиям заказчика.

Типовая подсистема защиты от угроз несанкционированного доступа

Применяемые элементы системы защиты информации от несанкционированного доступа направлены на решение таких задач, как:

- разграничение доступа к информационным ресурсам рабочих мест сотрудников или серверов системы;
- регистрация и протоколирование событий безопасности;
- целостность программно-аппаратного обеспечения, используемого в ОТС при обработке информации.

Анализ предметной области показал, что основными элементами подсистемы защиты информации от несанкционированного доступа (НСД) являются (см. рис. 1):

- автоматизированные рабочие места;
- сертифицированные средства защиты.

При этом контролируется конфигурация и параметры настройки аппаратной и программной частей подсистемы.

В соответствии с целями функционирования ОТС формулируются задачи по обеспечению безопасности информации и реализуются соответствующие технические решения по защите рабочих мест и серверов от несанкционированного доступа. При этом целесообразно обращать внимание на такие структурно-важные параметры как:

- целостность защищаемой информации;
- форма регистрации событий безопасности.

Кроме того, в системе необходимо организовать контроль над выводом документов на печать и учет формируемых документов, защиту устройств ввода и вывода информации, а также обеспечить сбор данных из журналов событий для их дальнейшего анализа. На этой основе получен ряд типовых технических решений по построению элементов системы защиты информации в ОТС.

нированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, утв. Решением председателя Гостехкомиссии при Президенте РФ от 30 марта 1992 г.; Специальные требования и рекомендации по технической защите конфиденциальной информации от 30 августа 2002 г. (с изменениями, внесенными в соответствии с Извещениями о корректировке №1-2005, №1-2006, №1-2008). М.: Гостехкомиссия России, 2002.

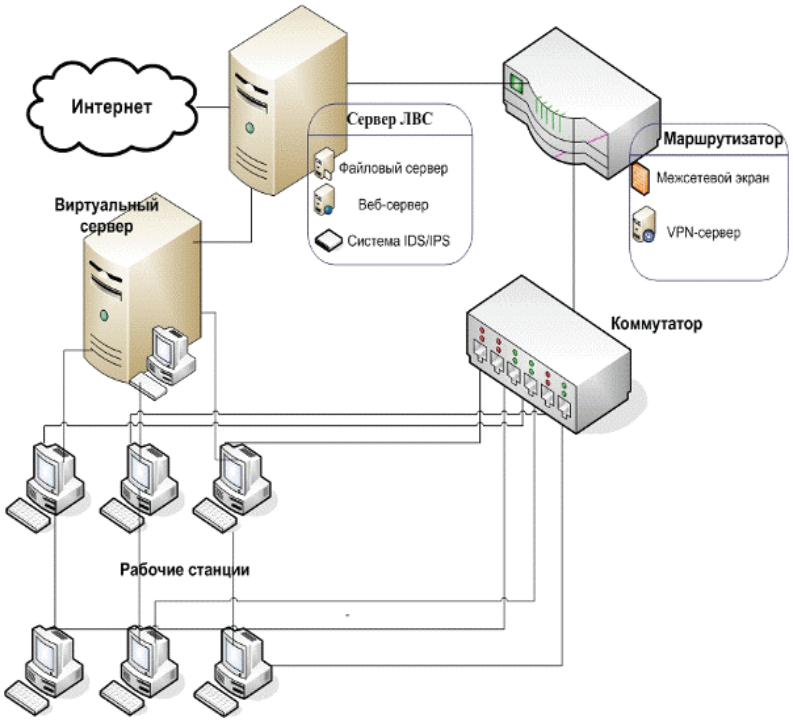

Рис. 2. Типовая структура подсистемы защиты информации от угроз вредоносного кода

Типовое техническое решение по созданию подсистемы защиты информации от НСД представлено на рис. 1. Структура подсистемы защиты обеспечивает выполнение требований нормативно-правовой документации в области защиты информации. В частности, «Положение о порядке обращения с информацией ограниченного распространения» обеспечивает организационную защиту информации, наряду с другими нормативными документами и должностными инструкциями, а также определяет общий порядок обращения с документами и материальными носителями информации, которые содержат информацию ограниченного доступа в организации. В «Положении…» определяется порядок обращения со служебной информацией, определяются ответственные лица, даются рекомендации по защите информации [2].

Типовая подсистема защиты информации от угрозы вредоносного кода

Подсистема защиты информации от вредоносного кода (подсистема антивирусной защиты) — это комплекс программно-технических средств и организационных решений [3] по обеспечению безопасности информации в ОТС.

В общем случае, типовая подсистема защиты информации от угроз вредоносного кода состоит из устройства управления соответствующим программным обеспечением (ПО) и самого ПО, устанавливаемого на рабочих местах сотрудников ОТС и серверах (рис. 2). Основными задачами, решаемыми такой подсистемой, являются: информирование пользователя об обнаружении факта воздействия вредоносного кода и управление средствами защиты информации.

Типовая подсистема межсетевого экранирования и защиты каналов передачи информации

Основным функциональным назначением существующих и разрабатываемых подсистем межсетевого экранирования и защиты каналов передачи информации является выполнение требований нормативно-правовых документов по разграничению доступа персонала к информационным ресурсам ОТС, а также их защита от сетевых атак, в частности, на основе применения скрытых (нетрадиционных) каналов [8, 11, 14, 15], и криптозащита сетевого трафика, связывающего подсистемы ОТС с внешними информационными системами и ресурсами [4].

Типовой состав подсистемы межсетевого экранирования и криптографической защиты каналов передачи информации включает в себя: межсетевые экраны; сегментообразующие коммутаторы; криптошлюзы (рис. 3).

Анализ назначения перечисленных элементов подсистемы межсетевого экранирования и криптографической защиты каналов передачи информации позволил сделать следующие выводы:

- основное назначение межсетевого экрана — контроль состояний сессий с применением процедуры фильтрации, а также реализация функции защиты информации от удаленного несанкционированного доступа и иных угроз сетевой безопасности [7];
- криптошлюзы обеспечивают функционирование VPN-туннелей между компьютерными сетями, используемыми в ОТС при передаче информации;
- рабочее место администратора подсистемы межсетевого экранирования и криптографической защиты каналов передачи информации реализует функции управления разграничением доступа к информаци-

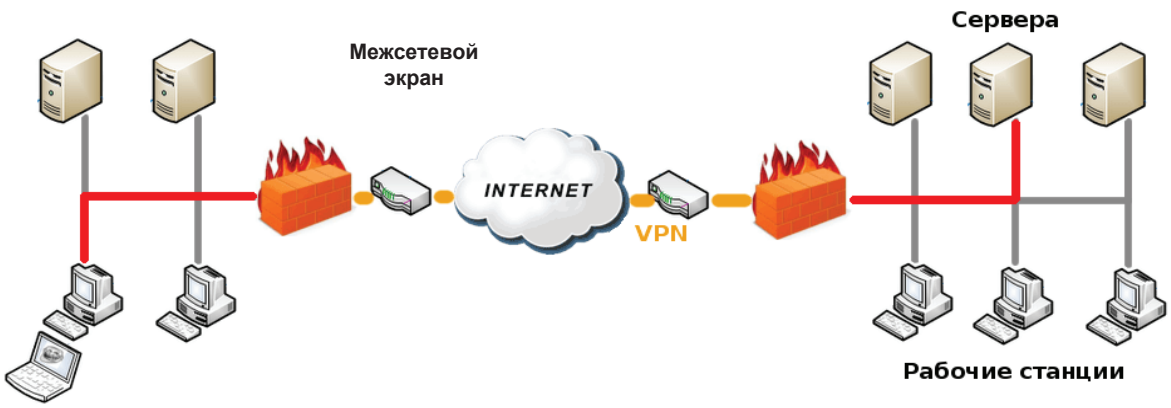

Рис. 3. Типовая структура подсистемы межсетевого экранирования и защиты каналов передачи информации

онным ресурсам ОТС, защиты информационных ресурсов от сетевых атак и взаимодействия с внешними информационными системами и ресурсами.

Таким образом, основной функцией межсетевого экранирования и криптозащиты каналов передачи информации является фильтрация сетевого трафика с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов [5].

Типовая подсистема анализа защищенности информации

Подсистема анализа защищенности информации предназначена для выявления и устранения возможностей реализации угроз нарушения защищенности информации, обрабатываемой в ОТС (рис. 4).

Как правило, выявление таких мест осуществляется путем сканирования узлов сети и сравнением результатов сканирования с известными данными об уязвимостях.

Типовая подсистема анализа защищенности — это комплекс программно-технических средств и организационных решений, обеспечивающих функции обнаружения уязвимостей программно-аппаратной части информационной подсистемы ОТС.

Возможных вариантов конфигурации типовой подсистемы анализа защищенности информации два: сертифицированный или несертифицированный сканер безопасности.

При выборе конфигурации системы не следует забывать о необходимости сертификации аппаратуры и, соответственно, оформления нормативно-правовой документации. С другой стороны, применение несертифицированного сканера безопасности предоставляет пользователю возможность преодоления ограничений, связанных с применением сертифицированных средств безопасности, а также появляется возможность обеспечения более высокого уровня обнаружения уязвимостей в программно-аппаратной части [6].

Анализ показал, что наиболее эффективным видом работ с использованием сканера безопасности является обнаружение различных уязвимостей в элементах компьютерной сети, которые могут быть использованы для доступа к информации ОТС и нарушения ее работы.

При применении сканера безопасности следует руководствоваться требованиями, определенными в «Положении о порядке организации и проведения работ по защите конфиденциальной информации». В соответствии с этим документом в ОТС определяются обязанности персонала, работающего с информацией, и ответственность за ее разглашение, а также порядок обращения с документами, содержащими информацию ограниченного распространения.

Особое внимание следует уделять учету электронных документов, которые содержат информацию ограниченного доступа.

Типовая подсистема обнаружения вторжения

Основным назначением предлагаемых к внедрению подсистем обнаружения вторжений является предотвращение сетевых атак, как на уровне локальной сети ОТС, так и на уровне операционных систем рабочих мест и серверов.

Современные системы обнаружения атаки на информационную часть ОТС способны обеспечить как защиту от угрозы сетевых атак, так и обнаружение иных попыток реализации угроз удаленного доступа [9], а также возможность аудита всех зарегистрированных событий.

Подсистема обнаружения вторжений — это комплекс программно-технических средств и организационных решений, обеспечивающих функции контроля сетевого трафика с целью обнаружения угроз удаленного доступа и сетевых атак на защищаемые информационные ресурсы системы[3] (рис. 5).

Типовая структура подсистемы обнаружения вторжений включает в себя средства обнаружения атак на уровнях: сети; операционных систем рабочих мест персонала и серверов; сетевых узлов.

Типовая подсистема мониторинга событий безопасности

Подсистема мониторинга событий безопасности в информационной подсистеме ОТС предназначена для

[3] *См.:* Организационно-правовое обеспечение информационной безопасности: Учеб. пособие / Под ред. А. А. Семененко. М.: МГИУ, 2014. 215 с.

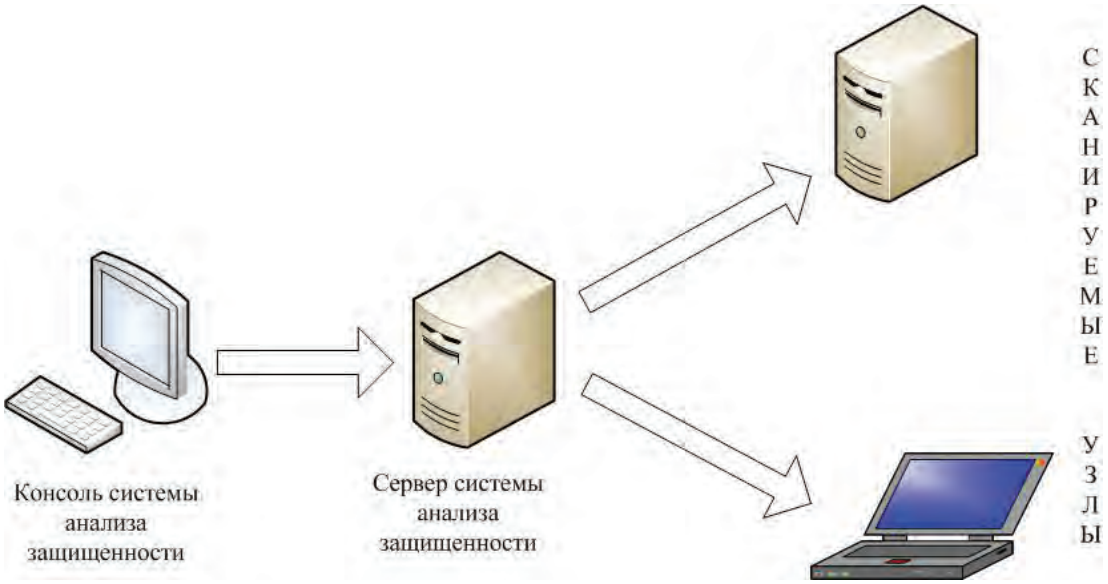

Рис. 4. Типовая структура подсистемы анализа защищенности информации

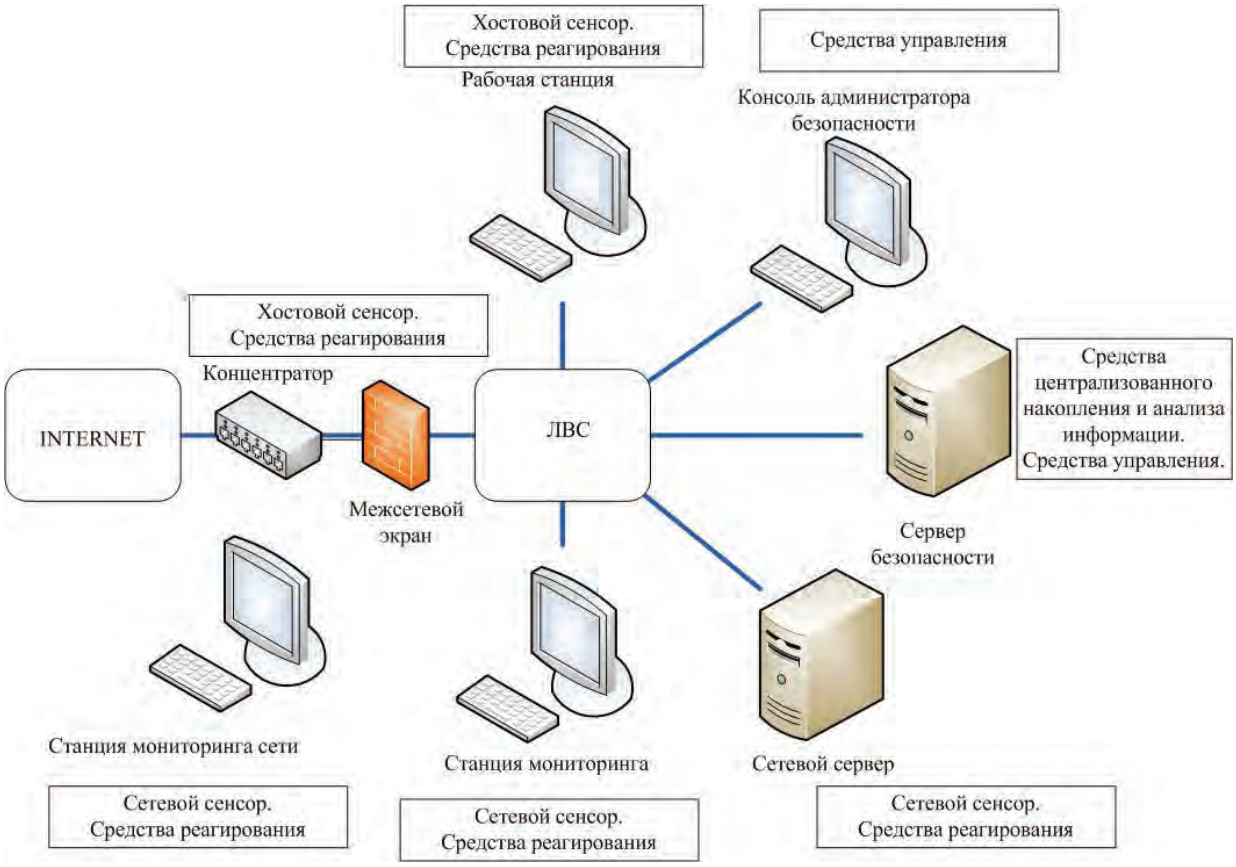

Рис. 5. Типовая структура подсистемы обнаружения вторжений

осуществления комплексного контроля за процессами функционирования общего и специального программного обеспечения, применяемого в ОТС[4] (рис. 6).

Для эффективной организации мониторинга событий безопасности в ОТС необходимо классифицировать эти события. Анализ предметной области показал, что сегодня события безопасности группируются в следующие классы:

– события безопасности, соотнесенные к входу/выходу элемента компьютерной сети, т. е. в соответствующую часть общего или специального программного обеспечения;

[4] *См.:* Организационно-правовое обеспечение информационной безопасности: Учеб. пособие / Под ред. А. А. Стрельцова. М. : ИЦ «Академия», 2013. 256 с.

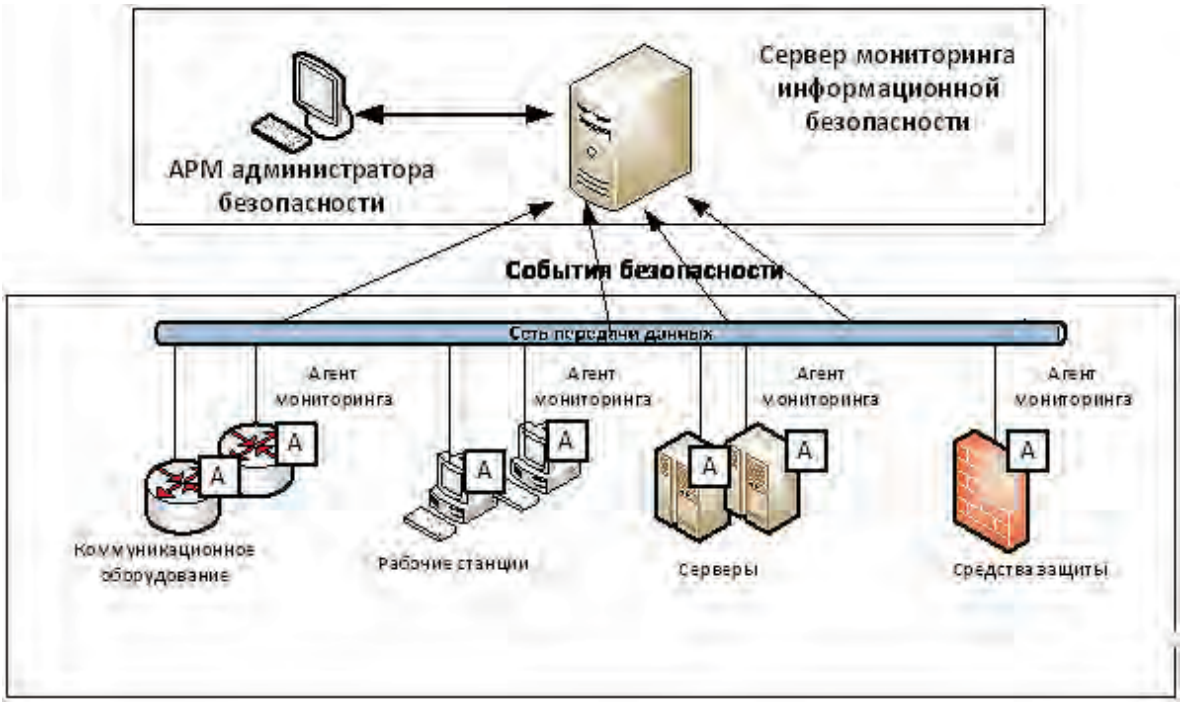

Рис. 6. Типовая структура подсистемы мониторинга событий безопасности

- события безопасности, инициируемые в процессе запуска соответствующего программного обеспечения;
- события безопасности, инициируемые в процессе выполнения программ;
- события безопасности, инициируемые при регистрации проявлений и блокирования сетевых атак [13].

Заключение

Стратегия ОТС в области информационной безопасности определяет принятие соответствующих мер для защиты информации от различных видов воздействия, и, как следствие, состав системы защиты информации.

Известно, что цели ОТС не могут быть выполнены без своевременного обеспечения сотрудников информацией, необходимой для выполнения должностных обязанностей. В этой связи, основой для построения эффективной системы защиты информации в ОТС как программно-технической и организационной системы является соответствующая нормативно-правовая документация. В положениях нормативно-правовых документов определены требования, необходимые для разработки соответствующих должностных инструкций, определяющих действия сотрудников, имеющих доступ к важной информации, а также состав самой системы защиты информации.

Таким образом, правовое обеспечение при построении системы защиты информации в ОТС имеет если не главное, то определяющее значение. Предварительный учет требований нормативно-правовых документов по обеспечению защиты, в том числе и информации в ОТС, позволяет более точно определить структуру и параметры системы защиты привилегированной информации.

Рецензент: ***Цимбал Владимир Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, профессор кафедры автоматизированных систем управления Филиала военной академии имени Петра Великого, г. Серпухов, Российская Федерация.*
E-mail: tsimbalva@mail.ru

Литература

1. Анин Б. Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
2. Барсуков В. С., Водолазний В. В. Современные технологии безопасности. М. : «Нолидж», 2014. 496 с.
3. Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А. Основы информационной безопасности. М. : Гор. линия — Телеком, 2018. 544 с.

4. Воронов А. В. Вопросы построения системы защиты информации: методологические аспекты // Жизнь и безопасность. 2012. № 3. С. 354—358.
5. Галатенко В. А. Основы информационной безопасности / Под. ред. В. Б. Бетелина. М. : ИНТУИТ, 2003. 277 с.
6. Ларин Д. А., Баранова Е. К., Бабаш А. В. Информационная безопасность. История защиты информации в России. М. : Изд-во: КДУ, 2015. 736 с.
7. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
8. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
9. Ловцов Д. А. Проблема информационной безопасности ГАС РФ «Правосудие» // Российское правосудие. 2012. № 5. С. 103—109.
10. Ловцов Д. А. О парадигме информационной безопасности эргасистем // Вопросы защиты информации. 2001. № 4. С. 20—25.
11. Ловцов Д. А. Информационная безопасность эргасистем: нетрадиционные угрозы, методы, модели // Информация и космос. 2009. № 4. С. 100—105.
12. Ловцов Д. А., Верхоглядов А. А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. 2008. № 8. С. 55— 64.
13. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М. : ДМК, 2017. 448 с.
14. Ловцов Д. А., Ермаков И. В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // НТИ. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1—7.
15. Ловцов Д. А., Ермаков И. В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1—9.

A LEGAL APPROACH TO BUILDING AN INFORMATION PROTECTION SYSTEM IN AN ORGANISATION

Vladimir Alekseev, *Dr.Sc. (Technology), Professor, Corresponding Member of the Russian Academy of Natural Sciences, Honoured Radio Operator of the Russian Federation, Head of the Department of Information Systems and Information Protection of the Tambov State Technical University, Russian Federation, Tambov.*
E-mail: vvalex1961@yandex.ru

Evgenii Emel'ianov, *Ph.D. student at the Federal Centre for Science and High Technologies "SNPO Eleron", Russian Federation, Moscow.*
E-mail: evemelyanov@rosatom.ru

Dmitrii Kasterin, *operator of the research unit of the Interbranch Centre for Training and Combat Use of Electronic Warfare Troops of the Russian Federation, Tambov.*
E-mail: dmitkast1996@mail.ru

Aleksei Strel'tsov, *Ph.D. student at the Federal Centre for Science and High Technologies "SNPO Eleron", Russian Federation, Moscow.*
E-mail: alastreltsov@rosatom.ru

Keywords: *information, privileged information, legal support, information security, threats, protection system, typical structure, legal regulations, organisational and technical system.*

Abstract.

Purpose of the work: *studying the relationships between the stages of building an information protection system in an organisation taking into account appropriate groups of legal regulations and legislative acts.*

Method used: *the authors guided by the systemic approach tried to trace the extent of impact of the requirements of certain legal regulations and legislative acts on the decisions taken by developers as regards the composition and relationships of elements of the information protection system within an organisation.*

Results obtained: *a number of generalised technical solutions for the configuration of elements of the information protection system in an organisation are proposed. The main result of the study should be considered the conclusion that legal support is important in building the information protection system of an organisational and technical system, and considering in advance the requirements of the legal regulations on information protection allows to more precisely determine its structure and parameters.*

References

1. Anin B. Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016, 384 pp.
2. Barsukov V. S., Vodolaznii V. V. Sovremennye tekhnologii bezopasnosti. M. : "Nolidzh", 2014, 496 pp.
3. Belov E. B., Los' V. P., Meshcheriakov R. V., Shelupanov A. A. Osnovy informatsionnoi bezopasnosti. M. : Gor. liniia -- Telekom, 2018, 544 pp.
4. Voronov A. V. Voprosy postroeniia sistemy zashchity informatsii: metodologicheskie aspekty. Zhizn' i bezopasnost', 2012, No. 3, pp. 354-358.
5. Galatenko V. A. Osnovy informatsionnoi bezopasnosti. Pod. red. V. B. Betelina. M. : INTUIT, 2003, 277 pp.
6. Larin D. A., Baranova E. K., Babash A. V. Informatsionnaia bezopasnost'. Istoriia zashchity informatsii v Rossii. M. : Izd-vo: KDU, 2015, 736 pp.
7. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
8. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74, DOI: 10.21681/1994-1404-2017-3-66-74.
9. Lovtsov D. A. Problema informatsionnoi bezopasnosti GAS RF "Pravosudie". Rossiiskoe pravosudie, 2012, No. 5, pp. 103-109.
10. Lovtsov D. A. O paradigme informatsionnoi bezopasnosti ergasistem. Voprosy zashchity informatsii, 2001, No. 4, pp. 20-25.
11. Lovtsov D. A. Informatsionnaia bezopasnost' ergasistem: netraditsionnye ugrozy, metody, modeli. Informatsiia i kosmos, 2009, No. 4, pp. 100-105.
12. Lovtsov D. A., Verkhogliadov A. A. Informatsionnaia bezopasnost' sudebnykh avtomatizirovannykh informatsionnykh sistem: pravovoe regulirovanie i iurisdiktsiia. Rossiiskoe pravosudie, 2008, No. 8, pp. 55- 64.
13. Petrov A. A. Komp'iuternaia bezopasnost'. Kriptograficheskie metody zashchity. M. : DMK, 2017, 448 pp.
14. Lovtsov D. A., Ermakov I. V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. NTI, Ser. 2. Inform. protsessy i sistemy, 2005, No. 2, pp. 1-7.
15. Lovsov D. A., Ermakov I. V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI, Ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1-9.