

Краснодарский университет МВД России

**УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ**

Учебное пособие

Краснодар
2019

УДК 004.056
ББК 32.973.26-018.2
У66

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *С. Г. Ключев, А. Б. Сизоненко*

Рецензенты:

Е. С. Поликарпов, кандидат технических наук (Московский университет МВД России имени В.Я. Кикотя);

М. В. Коцарев (Главное управление МВД России по Краснодарскому краю).

Управление информационной безопасностью : учебное
У66 пособие / сост. : С. Г. Ключев, А. Б. Сизоненко. – Краснодар : Краснодарский университет МВД России, 2019. – 224 с.

ISBN 978-5-9266-1508-8

Содержится понятийный аппарат, показаны основы управления информационной безопасностью органов внутренних дел Российской Федерации. Рассмотрены вопросы управления рисками информационной безопасности. Представлены наиболее важные аспекты управления инцидентами информационной безопасности.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 004.056
ББК 32.973.26-018.2

ISBN 978-5-9266-1508-8

© Краснодарский университет
МВД России, 2019
© Ключев С. Г., Сизоненко А. Б.,
составление, 2019

ВВЕДЕНИЕ

Информация – это актив, который, подобно другим активам органа внутренних дел или организации системы МВД России, имеет ценность и, следовательно, должен быть защищен надлежащим образом. Информационные процессы активно воздействуют на все стороны основных направлений деятельности органов внутренних дел. Использование новейших информационных технологий многократно усиливает это влияние. Как результат такого влияния – информация в настоящее время подвергается растущему числу и более широкому спектру угроз и уязвимостей.

Информация может существовать в различных формах: быть напечатанной или написанной на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или выражена устно. Независимо от формы представления информации, средств ее распространения или хранения, она всегда должна быть адекватно защищена.

Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности служебной деятельности органов внутренних дел и минимизации риска воздействия на них со стороны преступного сообщества.

Информационная безопасность органов внутренних дел достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств. Указанные меры и средства контроля и управления необходимо создавать, реализовывать, подвергать мониторингу, анализировать и улучшать, если необходимо, для обеспечения уверенности в том, что определенная безопасность и определенные цели служебной деятельности достигнуты. Все это необходимо выполнять наряду с другими процессами управления органами внутренних дел.

Информация и поддерживающие ее процессы, системы и сети являются важными служебными активами. Определение, достижение, поддержка и улучшение информационной безопасно-

сти могут быть существенными аспектами для поддержания устойчивости и непрерывности служебной деятельности органов внутренних дел, соблюдения законности и поддержания высокого имиджа Министерства внутренних дел Российской Федерации.

Органы внутренних дел и организации системы МВД России (далее – органы внутренних дел), а также их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, пожар или наводнение. Источники ущерба, например вредоносный код, компьютерное хакерство и атаки типа отказа в обслуживании, становятся более распространенными и все более и более изощренными.

Взаимодействие сетей общего пользования и совместное использование информационных ресурсов приводит к увеличению трудностей, связанных с управлением доступом к информации. Тенденция к использованию распределенной обработки данных также ослабляет эффективность централизованного контроля.

При проектировании многих информационных систем проблемы безопасности не учитывались. Уровень безопасности, который может быть достигнут техническими средствами, имеет ряд ограничений и, следовательно, должен поддерживаться надлежащим управлением и процессами. Выбор необходимых мер и средств контроля и управления требует тщательного планирования и внимания к деталям. Управление информационной безопасностью нуждается, как минимум, в участии всех сотрудников органа внутренних дел или организации.

Настоящее учебное пособие может, наряду с учебным процессом по специальности 10.05.05, также быть использовано в практической деятельности территориальных органов внутренних дел и расцениваться как методические рекомендации для разработки и внедрения системы управления информационной безопасностью органа внутренних дел.

Для большего удобства работы с настоящим учебным пособием все меры и средства контроля и управления в тексте выделяются жирным шрифтом и курсивом. Например: ***Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников органа внутренних дел и соответствующих сторонних орга-***

низаций. После которой приводятся рекомендация по их реализации.

Дополнительная информация, требующая внимания и анализа, в тексте настоящего пособия будет выделена большим восклицательным знаком. Например:

Могут быть установлены соглашения на совместное использование информации с целью улучшения сотрудничества и координации по вопросам безопасности. В таких соглашениях должны быть определены требования в отношении защиты чувствительной информации.

!

1. ОБЩИЕ ПОЛОЖЕНИЯ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

1.1. Основные термины и определения в области управления информационной безопасностью

В настоящем учебном пособии введены и применены следующие термины в области управления информационной безопасностью органов внутренних дел с соответствующими определениями:

контроль доступа – обеспечение того, чтобы доступ к активам был санкционирован и ограничен в соответствии с требованиями нормативных правовых актов, условиями служебной деятельности и безопасности;

подотчетность – ответственность субъекта за его действия и решения;

актив – что-либо, что имеет ценность для организации¹;

атака – попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования;

аутентификация – обеспечение гарантии того, что заявленные характеристики объекта правильны;

подлинность – свойство, гарантирующее, что субъект или ресурс идентичен заявленному;

доступность – свойство быть доступным и готовым к использованию по запросу авторизованного субъекта;

обеспечение непрерывности основных направлений деятельности – процессы и/или процедуры, обеспечивающие уверенность в непрерывности выполнения основных направлений деятельности;

¹ Имеются различные типы активов:

- информация;
- программное обеспечение;
- материальные активы, например компьютер;
- услуги;
- люди и их квалификация, навыки и опыт;
- нематериальные активы, такие как репутация и имидж.

конфиденциальность – свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;

мера и средство контроля и управления¹ – средство для осуществления управления риском, включающее политики, процедуры, рекомендации, практические приемы или организационные структуры, которые могут иметь административный, технический, управленческий или правовой характер;

цель применения мер и средств контроля и управления – формулировка, характеризующая, чего следует достичь в результате реализации мер и средств контроля и управления;

корректирующее действие – действие по устранению причины несоответствия или другой нежелательной ситуации;

эффективность – связь между достигнутым результатом и тем, насколько целесообразно использованы ресурсы;

результативность – степень реализации запланированной деятельности и достижения запланированных результатов;

событие – возникновение специфического набора обстоятельств;

воздействие – неблагоприятное изменение уровня достигнутых результатов основных направлений деятельности;

информационный актив – знания или данные, которые имеют значение для органа внутренних дел или организации;

информационная безопасность² – сохранение конфиденциальности, целостности и доступности информации;

событие в системе информационной безопасности – выявленное состояние системы, сервиса или состояние сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности информации;

инцидент информационной безопасности – одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной степенью вероят-

¹ Термин «мера и средство контроля и управления» также используется как синоним терминов «защитная мера» или «контрмера».

² Также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность.

ности приводят к компрометации операций основных направлений деятельности и создают угрозы для информационной безопасности. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа;

управление инцидентами информационной безопасности – процессы обнаружения, информирования, оценки, реагирования, рассмотрения и изучения инцидентов информационной безопасности;

система управления информационной безопасности – часть общей системы управления, основанная на анализе рисков основных направлений деятельности и предназначенная для создания, внедрения, функционирования, мониторингу, анализу, поддержке и улучшению информационной безопасности;

риск информационной безопасности – потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для органа внутренних дел и/или организации;

целостность – свойство сохранения правильности и полноты активов;

система управления – система, включающая в себя политики, процедуры, рекомендации и связанные с ними ресурсы для достижения целей основных направлений деятельности;

неотказуемость – способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение;

политика – общее намерение и направление, официально выраженное руководством;

предупреждающее действие – действие, предпринятое для устранения потенциального несоответствия или другой потенциально нежелательной ситуации;

процедура – установленный способ действия или процесса;

процесс – совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы;

достоверность – свойство соответствия предусмотренному поведению и результатам;

риск – сочетание вероятности события и его последствий;

принятие риска – решение принять риск;

анализ риска¹ – систематическое использование информации для выявления источников и оценки риска;

оценка риска – общий процесс анализа риска и оценивания риска;

коммуникация риска – обмен информацией о риске или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами;

критерии риска – правила, по которым оценивают значимость риска;

количественная оценка риска – процесс присвоения значений вероятности и последствий риска;

оценивание риска – процесс сравнения оценочной величины риска с установленным критерием риска с целью определения уровня значимости риска;

управление риском² – скоординированные действия по руководству и управлению органом внутренних дел и/или организацией в отношении риска;

обработка риска – процесс выбора и осуществления мер по модификации риска;

остаточный риск – риск, остающийся после его обработки;

угроза – возможная причина нежелательного инцидента, который может нанести ущерб системе или организации;

уязвимость – слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой;

¹ Анализ риска обеспечивает базу для оценивания риска, обработки риска и принятия риска.

² Управление риском обычно включает в себя оценку риска, обработку риска, принятие риска, коммуникацию риска, мониторинг риска и пересмотр риска.

1.2. Нормативно-правовое регулирование управления информационной безопасностью

1.2.1. Стандарты в области управления информационной безопасностью, используемые в Российской Федерации

Стандарты в области информационной безопасности имеют тенденцию к постоянному совершенствованию из-за непрерывного возникновения угроз информационной безопасности. В настоящее время в Российской Федерации используются следующие стандарты.

ГОСТ Р ИСО/МЭК 27000-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

ГОСТ Р ИСО/МЭК 27003-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27004-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

ГОСТ Р ИСО/МЭК 27006-2008. Национальный стандарт Российской Федерации. Информационная технология. Методы и

средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27007-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27011-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002.

ГОСТ Р ИСО/МЭК 27031-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности служебной деятельности.

ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.

ГОСТ Р ИСО/МЭК 27033-2-2012. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети.

ГОСТ Р ИСО/МЭК 27033-3-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

ГОСТ Р ИСО/МЭК 27034-1-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.

ГОСТ Р ИСО/МЭК 27037-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентифика-

ции, сбору, получению и хранению свидетельств, представленных в цифровой форме.

ГОСТ Р ИСО/МЭК 27038-2016. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Требования и методы электронного цензурирования.

1.2.2. Международные стандарты в области управления информационной безопасностью

ISO/IEC 27000 – Information security management systems – Overview and vocabulary.

ISO/IEC 27001 – Information technology – Security Techniques – Information security management systems - Requirements.

ISO/IEC 27002 - Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS.

ISO/IEC 27003 - Information security management system implementation guidance.

ISO/IEC 27004 - Information security management - Monitoring, measurement, analysis and evaluation.

ISO/IEC 27005 - Information security risk management.

ISO/IEC 27006 - Requirements for bodies providing audit and certification of information security management systems.

ISO/IEC 27007 - Guidelines for information security management systems auditing.

ISO/IEC TR 27008 - Guidance for auditors on ISMS controls.

ISO/IEC 27009 - Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the ISO27K standards.

ISO/IEC 27010 - Information security management for inter-sector and inter-organizational communications.

ISO/IEC 27011 - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.

ISO/IEC 27013 - Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.

ISO/IEC 27014 - Information security governance.

ISO/IEC TR 27015 - Information security management guidelines for financial services.

ISO/IEC TR 27016 - Information security economics.

ISO/IEC 27017 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO/IEC TR 27019 - Information security for process control in the energy industry.

ISO/IEC 27031 - Guidelines for information and communication technology readiness for business continuity.

ISO/IEC 27032 - Guideline for cybersecurity.

ISO/IEC 27033-1 - Network security - Part 1: Overview and concepts.

ISO/IEC 27033-2 - Network security - Part 2: Guidelines for the design and implementation of network security.

ISO/IEC 27033-3 - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues.

ISO/IEC 27033-4 - Network security - Part 4: Securing communications between networks using security gateways.

ISO/IEC 27033-5 - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs).

ISO/IEC 27033-6 - Network security - Part 6: Securing wireless IP network access.

ISO/IEC 27034-1 - Application security - Part 1: Guideline for application security.

ISO/IEC 27034-2 - Application security - Part 2: Organization normative framework.

ISO/IEC 27034-6 - Application security - Part 6: Case studies.

ISO/IEC 27035-1 - Information security incident management - Part 1: Principles of incident management.

ISO/IEC 27035-2 - Information security incident management - Part 2: Guidelines to plan and prepare for incident response.

ISO/IEC 27036-1 - Information security for supplier relationships - Part 1: Overview and concepts.

ISO/IEC 27036-2 - Information security for supplier relationships - Part 2: Requirements.

ISO/IEC 27036-3 - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security.

ISO/IEC 27036-4 - Information security for supplier relationships - Part 4: Guidelines for security of cloud services.

ISO/IEC 27037 - Guidelines for identification, collection, acquisition and preservation of digital evidence.

ISO/IEC 27038 - Document redaction.

ISO/IEC 27039 - Intrusion prevention.

ISO/IEC 27040 - Storage security.

ISO/IEC 27041 - Investigation assurance.

ISO/IEC 27042 - Analyzing digital evidence.

ISO/IEC 27043 - Incident investigation.

ISO/IEC 27050-1 - Electronic discovery - Part 1: Overview and concepts.

ISO 27799 - Information security management in health using ISO/IEC 27002 - guides health industry organizations on how to protect personal health information using ISO/IEC 27002.

2. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

2.1. Политика информационной безопасности

Цель: Обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями служебной деятельности и соответствующими нормативными правовыми актами.

Высшее руководство должно установить четкое направление политики в соответствии с целями служебной деятельности и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках органа внутренних дел или организации.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

2.1.1. Документирование политики информационной безопасности

Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников органа внутренних дел и соответствующих сторонних организаций.

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. Документ, в котором излагается политика, должен содержать положения относительно:

а) определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б) изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями служебной деятельности;

в) подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и управление риском;

г) краткого разъяснения наиболее существенных для органа внутренних дел политик безопасности, принципов, стандартов и требований соответствия, например:

- соответствие законодательным требованиям и договорным обязательствам;

- требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;

- управление непрерывностью служебной деятельности;

- ответственность за нарушения политики информационной безопасности;

д) определения общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах безопасности;

е) ссылок на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всего органа внутренних дел в актуальной, доступной и понятной форме.

Политика информационной безопасности может составлять часть документа по общей политике. Если политика информационной безопасности распространяется за пределами органа внутренних дел, следует принимать меры в отношении неразглашения чувствительной информации. Дополнительную информацию по данному вопросу можно найти в ГОСТ ИСО/МЭК 13335-1 [17].



2.1.2. Пересмотр политики информационной безопасности

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики безопасности. Пересмотр заключается в оценке возможностей по улучшению политики информационной безопасности органа внутренних дел и подхода к управлению информационной безопасностью в ответ на изменения организационной среды, обстоятельств служебной деятельности, правовых условий или технической среды.

При пересмотре политики информационной безопасности следует учитывать результаты пересмотров методов управления. Должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

Входные данные для пересмотра методов управления должны включать информацию об (о):

- а) ответной реакции заинтересованных сторон;
- б) результатах независимых пересмотров;
- в) состоянии предотвращающих и корректирующих действий;
- г) результатах предыдущих пересмотров методов управления;
- д) выполнении процесса и соответствии политике информационной безопасности;
- е) изменениях, которые могли бы повлиять на подход органа внутренних дел к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств служебной деятельности, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;
- ж) тенденциях в отношении угроз и уязвимостей;
- з) доведенных до сведения инцидентах информационной безопасности;

и) рекомендациях, данных соответствующими органами.

Выходные данные пересмотра методов управления должны включать любые решения и действия относительно:

а) улучшения подхода органа внутренних дел к управлению информационной безопасностью и ее процессов;

б) улучшения мер и средств контроля и управления и целей их применения;

в) улучшения распределения ресурсов и(или) обязанностей.

Пересмотр методов управления следует документировать. Пересмотренная политика должна быть утверждена руководством.

2.2. Организационные аспекты информационной безопасности

Цель: Осуществлять управление информационной безопасностью в рамках органа внутренних дел.

Должна быть создана структура управления для инициирования и контроля обеспечения информационной безопасности в органе внутренних дел.

Высшее руководство должно утверждать политику информационной безопасности организации, назначать ответственных лиц в области политики информационной безопасности, а также координировать и анализировать внедрение информационной безопасности в органе внутренних дел.

При необходимости следует предусмотреть назначение должностного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с отдельными внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

2.2.1. Обязательства руководства по отношению к информационной безопасности

Руководству следует активно поддерживать безопасность в организации с помощью четкого управления, видимого распределения обязанностей, определенных назначений и признания обязанностей в отношении информационной безопасности.

Руководству следует:

а) обеспечивать уверенность в том, что цели информационной безопасности определены, соответствуют требованиям органа внутренних дел и включены в соответствующие процессы;

б) формулировать, анализировать и утверждать политику информационной безопасности;

в) анализировать эффективность реализации политики информационной безопасности;

г) обеспечивать четкое управление и очевидную поддержку управления в отношении инициатив, связанных с безопасностью;

д) обеспечивать ресурсы, необходимые для информационной безопасности;

е) утверждать определенные роли и ответственности в отношении информационной безопасности в рамках органа внутренних дел;

ж) инициировать планы и программы для поддержки осведомленности об информационной безопасности;

з) обеспечивать уверенность в том, что реализация мер и средств контроля и управления информационной безопасностью скоординирована в рамках органа внутренних дел.

Руководству следует определять потребность в консультациях с внутренними или внешними специалистами по информационной безопасности, а также анализировать и координировать результаты консультаций в рамках органа внутренних дел.

В зависимости от величины органа внутренних дел такие обязанности могут выполняться соответствующим коллегиальным органом управления, например экспертной комиссией по режиму секретности.

2.2.2. Координация вопросов информационной безопасности

Деятельность, связанная с информационной безопасностью, должна быть скоординирована представителями различных подразделений органа внутренних дел с соответствующими ролями и должностными обязанностями.

Как правило, координация проблем информационной безопасности должна включать в себя сотрудничество и участие руководителей, пользователей, администраторов, разработчиков прикладных программ, аудиторов и сотрудников, занимающегося безопасностью, а также специалистов в области правовых аспектов, кадровых ресурсов, ИТ или управления риском.

Такая деятельность должна:

а) обеспечивать уверенность в том, что обеспечение безопасности осуществляется в соответствии с политикой информационной безопасности;

б) определять способ устранения несоответствия;

в) утверждать методики и процессы обеспечения информационной безопасности, например оценку риска, классификацию информации;

г) выявлять значительные изменения угроз и подверженность информации и средств обработки информации угрозам;

д) оценивать адекватность и координировать реализацию мер и средств контроля и управления информационной безопасностью;

е) эффективно способствовать осведомленности, обучению и тренингу в отношении информационной безопасности в рамках органа внутренних дел;

ж) оценивать информацию, полученную в результате мониторинга и анализа инцидентов информационной безопасности, и рекомендовать соответствующие действия в ответ на выявленные инциденты информационной безопасности.

Если в органе внутренних дел не используется специальная межфункциональная группа, например по причине несоответствия величине органа внутренних дел, вышеописанные действия могут выполняться другим подходящим органом управления или отдельным должностным лицом.



2.2.3. Распределение обязанностей по обеспечению информационной безопасности

Все обязанности по обеспечению информационной безопасности должны быть четко определены.

Распределение обязанностей по обеспечению информационной безопасности следует осуществлять в соответствии с политикой информационной безопасности. Следует четко определять обязанности по защите отдельных активов и по выполнению конкретных процессов, связанных с информационной безопасностью. Такие обязанности следует дополнять, при необходимости, более детальными руководствами для конкретных мест эксплуатации и средств обработки информации. Конкретные обязанности в отношении защиты активов и осуществления специфических процессов, связанных с безопасностью, например планирование непрерывности служебной деятельности, должны быть четко определены.

Лица, на которые возложена обязанность по обеспечению безопасности, могут делегировать задачи, связанные с безопасностью, другим лицам. Тем не менее, они остаются ответственными за выполнение делегированных задач.

Круг обязанностей каждого руководителя должен быть четко определен, в частности:

- а) активы и процессы (процедуры) безопасности, связанные с каждой конкретной системой, должны быть четко определены;
- б) необходимо назначить ответственных за каждый актив или процедуру безопасности, и подробно описать их обязанности в соответствующих документах;
- в) уровни полномочий должны быть четко определены и документально оформлены.

Во многих органах внутренних дел назначается на подразделения информационных технологий, связи и защиты информации возлагается общая ответственность за разработку и реализацию безопасности и за поддержку определения мер и средств контроля и управления.

Однако обязанности в отношении поиска ресурсов и реализации мер и средств контроля и управления часто вменяются отдельным руководителям. Общепринятой практикой является назначение ответственного для каждого актива, который несет ответственность за его повседневную защиту.



2.2.4. Процесс получения разрешения на использование средств обработки информации

Необходимо определить и реализовать процесс получения разрешения у руководства на использование новых средств обработки информации.

В отношении процесса получения разрешения следует рассмотреть следующие рекомендации:

а) на новые средства должны быть получены соответствующие разрешения руководства пользователей, утверждающего их цель и использование. Разрешение следует также получать от руководителя, ответственного за поддержку среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие требования и политики безопасности соблюдаются;

б) аппаратные средства и программное обеспечение, где необходимо, следует проверять на предмет совместимости с другими компонентами системы;

в) использование персональных или находящихся в частной собственности средств обработки информации, например ноутбуков, домашних компьютеров или карманных устройств для обработки служебной информации может являться причиной новых уязвимостей, поэтому следует определять и реализовывать необходимые меры и средства контроля и управления.

2.2.5. Соглашения о конфиденциальности

Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности органа внутренних дел в защите информации, должны определяться и регулярно пересматриваться.

В соглашениях о конфиденциальности или неразглашении должно содержаться требование о защите охраняемой законом информации, выраженное юридическими терминами, имеющими исковую силу. Чтобы определить требования для соглашений о конфиденциальности или неразглашении, необходимо учесть следующие факторы:

а) определение информации, подлежащей защите (например, тайна следствия);

б) предполагаемый срок действия соглашения, включая случаи, когда может возникнуть необходимость в неограниченной поддержке конфиденциальности;

в) необходимые действия при окончании срока действия соглашения;

г) обязанности и действия лиц, подписавших соглашение, с целью предотвращения несанкционированного разглашения информации (например по принципу «необходимого знания»);

д) разрешенное использование охраняемой законом информации и права лиц, подписавших соглашение, в отношении использования информации;

е) право подвергать аудиту и мониторингу деятельность, связанную с защищаемой информацией;

ж) процедуру предупреждения и сообщения о несанкционированном разглашении или нарушениях, связанных с защищаемой информацией;

з) условия возврата или уничтожения информации в случае приостановления действия соглашения;

и) предполагаемые действия, которые должны быть приняты в случае нарушения данного соглашения.

В зависимости от требований безопасности органа внутренних дел, могут потребоваться дополнительные элементы соглашения о конфиденциальности или неразглашении.

Соглашения о конфиденциальности и неразглашении должны соответствовать всем применимым законам и нормам, под юрисдикцию которых они подпадают.

Требования в отношении соглашений о конфиденциальности и неразглашении должны пересматриваться периодически и когда происходят изменения, влияющие на эти требования.

Соглашения о конфиденциальности и неразглашении защищают информацию органа внутренних дел, а также информируют лиц, подписавших соглашение, об их обязанности защищать, использовать и разглашать информацию санкционированным способом.

При различных обстоятельствах органу внутренних дел могут потребоваться различные формы соглашений о конфиденциальности или неразглашении.



2.2.6. Контакт с различными инстанциями

Должны поддерживаться соответствующие контакты с различными инстанциями.

В органе внутренних дел должны применяться процедуры, определяющие, когда и с какими инстанциями (например правоохранительными, пожарными и надзорными органами) необходимо вступить в контакт, и каким образом следует своевременно сообщать о выявленных инцидентах информационной безопасности, если есть подозрение о возможности нарушения закона.

Органам внутренних дел, подвергающимся атаке через Интернет, может потребоваться привлечение внешней третьей стороны (например провайдера Интернет-услуг или телекоммуникационного оператора) для принятия мер против источника атаки.

При осуществлении таких контактов может потребоваться поддержка процесса управления инцидентами информационной безопасности или процесса планирования непрерывности служебной деятельности и действий в чрезвычайных ситуациях. Также следует поддерживать контакты с регулирующими органами для прогнозирования и подготовки к предстоящим изменениям в законах или нормах, которые должны соблюдаться органом внутренних дел.

Контакты с другими инстанциями включают контакты с коммунальными службами, скорой помощью и службами охраны труда, например с пожарными органами (в связи с непрерывностью служебной деятельности), провайдерами телекоммуникационных услуг (в связи с трассировкой линий связи и их доступностью), службами водоснабжения (в связи со средствами охлаждения оборудования).



2.2.7. Контакт со специализированными профессиональными группами

Должны поддерживаться соответствующие контакты со специализированными профессиональными группами или участниками форумов по безопасности, а также с профессиональными ассоциациями.

Членство в специализированных группах или форумах следует рассматривать как средство для:

а) повышения знания о «передовом опыте» и достижений информационной безопасности на современном уровне;

б) обеспечения уверенности в том, что понимание проблем информационной безопасности является современным и полным;

в) получения раннего оповещения в виде предупреждений, информационных сообщений и патчей¹ касающихся атак и уязвимостей;

г) возможности получения консультаций специалистов по вопросам информационной безопасности;

д) совместного использования и обмена информацией о новых технологиях, продуктах, угрозах или уязвимостях;

е) обеспечения адекватных точек контакта для обсуждения инцидентов информационной безопасности.

Могут быть установлены соглашения на совместное использование информации с целью улучшения сотрудничества и координации по вопросам безопасности. В таких соглашениях должны быть определены требования в отношении защиты чувствительной информации.



2.2.8. Независимая проверка информационной безопасности

Подход органа внутренних дел к управлению информационной безопасностью и ее реализации (т. е. цели управления, политики, процессы и процедуры по обеспечению информационной безопасности) должен проверяться независимым образом через запланированные интервалы времени, или когда произошли значительные изменения, связанные с реализацией безопасности.

Независимая проверка может инициироваться руководством. Такая независимая проверка необходима для обеспечения уверенности в сохраняющейся работоспособности, адекватности

¹ Патч – блок изменений для оперативного исправления или нейтрализации ошибки в исполняемой программе, чаще всего поставляемый (или размещаемый на сайте разработчика) в виде небольшой программы, вставляющей исправления в объектный код соответствующих модулей приложения. Иногда этот метод используется для добавления в приложение новой функциональности.

и эффективности подхода органа внутренних дел к управлению информационной безопасностью. Проверка должна включать в себя оценку возможностей улучшения и необходимость изменений подхода к безопасности, в том числе политику и цели управления.

Такая проверка должна осуществляться специалистами, не работающими в рассматриваемой области деятельности, например подразделением делопроизводства и режима или вышестоящим органом внутренних дел. Специалисты, привлекаемые к таким проверкам, должны обладать соответствующими навыками и опытом.

Результаты независимой проверки должны регистрироваться и сообщаться руководству, инициировавшему проверку. Эти отчеты необходимо сохранять для возможного последующего использования.

Если в результате независимой проверки устанавливается, что подход органа внутренних дел и реализация управления информационной безопасностью неадекватны или не соответствуют направлению информационной безопасности, изложенному в документе, содержащем политику информационной безопасности, руководству следует рассмотреть соответствующие корректирующие действия.

Область деятельности, которую необходимо регулярно проверять, может быть проверена независимым образом. Методы проверки могут включать опрос руководства, проверку данных регистрации или анализ документов, имеющих отношение к политике безопасности. ГОСТ Р ИСО 19011-2012 [18] также может предоставить полезное руководство по выполнению независимой проверки, включая создание и реализацию программы проверки.



2.3. Аспекты взаимодействия со сторонними организациями

Цель: Обеспечивать безопасность информации и средств обработки информации органа внутренних дел при доступе, обработке, передаче ее осуществляемого сторонними организациями.

Безопасность информации и средств обработки информации органа внутренних дел не должна снижаться при вводе продуктов или сервисов сторонних организаций.

Доступ сторонних организаций к средствам обработки информации органа внутренних дел, а также к обработке и передаче информации должен находиться под контролем.

Если имеется потребность служебной деятельности в работе со сторонними организациями, которым может потребоваться доступ к информации и средствам обработки информации органа внутренних дел, а также в получении или обеспечении продукта или сервиса от сторонней организации или для нее, следует выполнять оценку риска для определения последствий для безопасности и требований к мерам и средствам контроля и управления. Меры и средства контроля и управления следует согласовывать и определять в контракте со сторонней организацией

2.3.1. Идентификация рисков, являющихся следствием работы со сторонними организациями

Риски для информации и средств обработки информации органа внутренних дел, являющиеся следствием процессов служебной деятельности, в которых участвуют сторонние организации необходимо определять и реализовывать соответствующие меры и средства контроля и управления прежде, чем будет предоставлен доступ.

Там, где есть необходимость разрешения доступа сторонней организации к средствам обработки информации или информации органа внутренних дел, следует проводить оценку риска с целью определения каких-либо потребностей в специальных мерах и средствах контроля и управления. При определении рисков, связанных с доступом сторонних организаций, следует учитывать:

а) средства обработки информации, необходимые сторонним организациям для доступа;

б) тип доступа к информации и средствам обработки информации, который будет предоставлен сторонним организациям, например:

- физический доступ, например к служебным помещениям, машинным залам, картотекам;

- логический доступ, например к базам данных или информационным системам органа внутренних дел;

- возможность сетевого соединения между сетью (сетями) органа внутренних дел и сторонней организацией, например неразъемное соединение или удаленный доступ;

- осуществление доступа на месте или вне места эксплуатации;

в) ценность и чувствительность используемой информации, ее критичность для операций служебной деятельности;

г) меры и средства контроля и управления, необходимые для защиты информации, не предназначенной для доступа сторонним организациям;

д) персонал сторонней организации, участвующий в обработке информации органа внутренних дел;

е) каким образом организация или персонал, авторизованные на получение доступа, могут быть идентифицированы, авторизация проверена и как часто это необходимо подтверждать;

ж) различные способы и меры и средства контроля и управления, применяемые сторонними организациями при хранении, обработке, передаче, совместном использовании и обмене информацией;

з) влияние непредоставления требуемого доступа сторонней организации и ввода или получения сторонней организацией неточной или ложной информации;

и) инструкции и процедуры принятия мер в отношении инцидентов информационной безопасности и возможных убытков, а также сроки и условия возобновления доступа сторонних организаций в случае инцидента информационной безопасности;

к) правовые и нормативные требования, а также договорные обязательства, значимые для сторонних организаций, которые необходимо принимать в расчет;

л) влияние вышеназванных мер на интересы каких-либо других причастных сторон.

Доступ сторонних организаций к информации органа внутренних дел не должен обеспечиваться до тех пор, пока не будут реализованы соответствующие меры и средства контроля и управления и пока не будет подписан договор, определяющий сроки и условия подключения или доступа и рабочий механизм. Как правило, все требования к безопасности, вытекающие из работы со сторонними организациями или внутреннего контроля, должны отражаться в соглашении со сторонними организациями.

Следует обеспечивать уверенность в том, что сторонние организации осведомлены о своих обязанностях, и берут на себя ответственность и обязательства в отношении доступа, обработки, передачи или управления информацией и средств обработки информации органа внутренних дел.

Информация может быть подвергнута риску сторонними организациями, в которых управление информационной безопасностью осуществляется неадекватным образом. Должны определяться и применяться меры и средства контроля и управления с целью администрирования доступа сторонней организацией к средствам обработки информации. Например, там, где имеется определенная потребность в конфиденциальности информации, могут быть использованы соглашения о неразглашении.



Орган внутренних дел может сталкиваться с рисками, связанными с межорганизационными процессами, управлением и связью в том случае, если применяется большой процент аутсорсинга или если к участию привлекаются несколько сторонних организаций.

Меры и средства контроля и управления, приведенные выше охватывают различные мероприятия с привлечением сторонних организаций, включающие:

а) провайдеров услуг, например Интернет-провайдеров, сетевых провайдеров, услуги телефонной связи, технического обслуживания и поддержки;

б) аутсорсинг средств и (или) операций, например информационных систем;

в) разработчиков и поставщиков, например программных продуктов и информационных систем;

г) уборку, общественное питание и другие вспомогательные услуги, обеспечиваемые в рамках договоров аутсорсинга;

д) временных работников, прием на работу стажеров и другие нерегулярные краткосрочные назначения.

Такие соглашения могут помочь снизить риски, связанные с привлечением сторонних организаций.

2.3.2. Рассмотрение требований безопасности в договорах с третьей стороной

Договоры с третьей стороной, привлеченной к доступу, обработке, передаче или управлению информацией или средствами обработки информации органа внутренних дел, или к дополнению продуктов или услуг к средствам обработки информации, должны охватывать все соответствующие требования безопасности.

Договор должен обеспечивать уверенность в том, что нет никакого недопонимания между органом внутренних дел и третьей стороной. Орган внутренних дел должен убедиться, что третья сторона сможет возместить возможные убытки.

Следующие условия должны быть рассмотрены на предмет включения в договор с целью удовлетворения установленных требований безопасности:

- а) политика информационной безопасности;
- б) меры и средства контроля и управления для обеспечения уверенности в защите активов, включая:
 - процедуры по защите активов органа внутренних дел, в том числе информацию, программное обеспечение и аппаратные средства;
 - какие-либо меры и средства контроля и управления, а также инструменты необходимой физической защиты;
 - меры и средства контроля и управления для обеспечения уверенности в защите от вредоносного программного средства;
 - процедуры по определению компрометации активов, например вследствие потери или модификации информации, программного обеспечения и аппаратных средств;
 - меры и средства контроля и управления по обеспечению уверенности в возврате или уничтожении информации и активов по окончании договора или в согласованное время в течение срока действия договора;
 - конфиденциальность, целостность, доступность и любое другое значимое свойство активов;
 - ограничения на копирование и разглашение информации, и применение соглашений о конфиденциальности;

в) тренинг пользователей и администраторов в отношении методов, процедур и безопасности;

г) обеспечение осведомленности пользователей в отношении обязанностей и вопросов, связанных с информационной безопасностью;

д) обязанности, касающиеся установки и сопровождения аппаратных средств и программного обеспечения;

е) четкая структура подотчетности и согласованные форматы представления отчетов;

ж) ясный и определенный процесс управления изменениями;

з) политика управления доступом, охватывающая:

- различные причины, требования и преимущества, делающие доступ третьей стороны необходимым;

- разрешенные методы доступа, а также управление и использование уникальных идентификаторов пользователя и паролей;

- процесс авторизации в отношении доступа и привилегий пользователей;

- требование по ведению списка лиц, уполномоченных использовать предоставляемые услуги, с указанием соответствующих прав и привилегий;

- положение о том, что весь доступ, не авторизованный явным образом, является запрещенным;

- процесс отмены прав доступа или прерывание соединения между системами;

и) процедуры в отношении отчетности, уведомления и расследования инцидентов информационной безопасности и нарушений безопасности, а также нарушений требований, изложенных в соглашении;

к) описание продукта или услуги, которые должны быть предоставлены, и описание информации, которая должна быть предоставлена;

л) определение необходимого и неприемлемого уровня обслуживания;

м) определение поддающихся контролю критериев эффективности, а также их мониторинг и предоставление отчетности;

н) право на проведение мониторинга и отмену любой деятельности в отношении активов органа внутренних дел;

о) право на проведение аудита исполнения договорных обязательств и возможность проведения такого аудита третьей стороной, а также перечисление установленных законом прав аудиторов;

п) установление процесса информирования о возникающих проблемах с целью их разрешения;

р) требования в отношении непрерывности обслуживания, включая меры по обеспечению доступности и надежности, в соответствии с приоритетами служебной деятельности органа внутренних дел;

с) соответствующие обязательства сторон в рамках соглашения;

т) обязательства относительно юридических вопросов, и способов обеспечения уверенности в соответствии правовым требованиям, например законодательству о защите данных, особенно с учетом различных требований национальных правовых систем;

у) соблюдение прав на интеллектуальную собственность и авторских прав, а также обеспечение правовой защиты любой совместной работы;

ф) привлечение третьей стороны вместе с субподрядчиками, меры и средства контроля и управления безопасности, которые эти субподрядчики должны реализовать;

х) условия перезаключения/окончания договоров:

- план действий в чрезвычайных ситуациях должен содержать положения на случай, если какая-либо сторона пожелает прервать отношения до окончания срока действия договоров;

- перезаключение договоров в случае изменения требований органа внутренних дел к безопасности;

- действующие документированные перечни активов, лицензий, договоров или связанных с ними прав.

Договоры могут варьироваться в значительной мере в отношении различных организаций и среди различных типов третьих сторон. Поэтому следует заботиться о включении в договоры всех определенных рисков и требований безопасности. При необходимости требуемые меры и средства контроля и управления, а также процедуры могут быть расширены в плане управления безопасностью.



Если управление информационной безопасностью осуществляется в рамках договоров аутсорсинга, то в договорах должно быть оговорено, каким образом третья сторона будет гарантировать поддержание адекватной безопасности, определенной оценкой риска, а также адаптацию к выявленным рискам и изменениям рисков.

Некоторые из различий между аутсорсингом и другими формами обеспечения услуг третьими сторонами включают в себя вопросы ответственности, планирование переходного периода и возможного срыва операций в течение данного периода, планирование мероприятий на случай непредвиденных ситуаций и тщательность проверок, а также сбор и управление информацией по инцидентам безопасности. Поэтому важно, чтобы орган внутренних дел планировал и управлял переходом к договорам аутсорсинга, и применял соответствующий процесс управления изменениями и перезаключением/окончанием действия договоров.

В договоре необходимо учитывать процедуры непрерывной обработки на случай, если третья сторона окажется неспособной поставлять свои услуги, для предотвращения какой-либо задержки в служебной деятельности органа внутренних дел до замены услуг.

В договорах с третьими сторонами могут участвовать также и другие стороны. Договоры, предоставляющие доступ третьим сторонам, должны содержать разрешение на привлечение других организаций, а также условия их доступа и участия.

Как правило, договоры разрабатываются, в первую очередь, органом внутренних дел. Иногда договор может быть разработан и предложен органу внутренних дел третьей стороной. Органу внутренних дел необходимо обеспечивать уверенность в том, что требования третьей стороны, изложенные в предлагаемых договорах, не оказывают излишнего влияния на его собственную безопасность.

2.3. Процессный подход

Современные стандарты в области управления информационной безопасностью предполагают использовать процессный подход для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы

управления информационной безопасностью органа внутренних дел (далее – СУИБ).

Для успешного функционирования орган внутренних дел должен определить и осуществить управление многочисленными видами деятельности. Деятельность, использующая ресурсы и управляемая в целях преобразования входов в выходы, может быть рассмотрена как процесс. Часто выход одного процесса непосредственно формирует вход для следующего процесса.

Использование внутри органа внутренних дел системы процессов наряду с идентификацией и взаимодействием этих процессов, а также управление процессами могут быть определены как «процессный подход».

Согласно процессному подходу применительно к управлению информационной безопасностью особую значимость для органа внутренних дел имеют следующие факторы:

- а) понимание требований информационной безопасности органа внутренних дел и необходимости установления политики и целей информационной безопасности;

- б) внедрение и использование мер управления для управления рисками информационной безопасности общих рисков органа внутренних дел;

- в) мониторинг и проверка производительности и эффективности системы управления информационной безопасностью;

- г) непрерывное улучшение системы управления информационной безопасностью, основанное на результатах объективных измерений.

В ГОСТ Р ИСО/МЭК 27001-2006 [2] представлена модель «Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов системы управления информационной безопасностью. На рисунке 1 показано, как система управления информационной безопасностью, используя в качестве входных данных требования информационной безопасности и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам. Рисунок 1 иллюстрирует также связи между процессами.

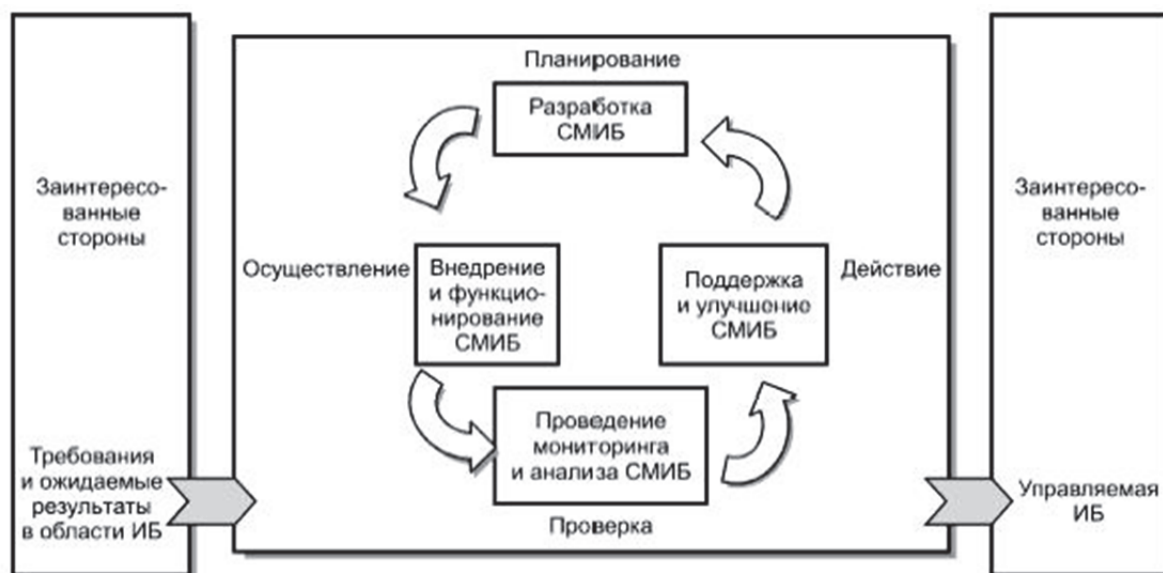


Рис. 1. Модель системы управления информационной безопасностью

Связи между процессами представлены также в таблице 1.

Таблица 1 Связи между процессами СУИБ

Планирование (разработка СУИБ)	Разработка политики, установление целей, процессов и процедур СУИБ, относящихся к управлению рисками и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям органа внутренних дел
Осуществление (внедрение и обеспечение функционирования СУИБ)	Внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СУИБ
Проверка (проведение мониторинга и анализа СУИБ)	Оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СУИБ и информирование высшего руководства о результатах для последующего анализа
Действие (поддержка и улучшение СУИБ)	Проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СУИБ

2.4. Система управления информационной безопасностью

Орган внутренних дел должен разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СУИБ применительно ко всей служебной деятельности органа внутренних дел и рискам, с которыми она сталкивается.

2.4.1. Разработка системы управления информационной безопасностью

Орган внутренних дел должен осуществить следующее:

а) определить область и границы действия СУИБ с учетом характеристик служебной деятельности, органа внутренних дел, его размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия;

б) определить политику СУИБ на основе характеристик служебной деятельности, органа внутренних дел, его размещения, активов и технологий, которая:

- содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;

- принимает во внимание требования служебной деятельности, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;

- согласуется со стратегическим содержанием управления рисками органа внутренних дел, в рамках которого будет разрабатываться и поддерживаться СУИБ;

- устанавливает критерии оценки рисков;

- утверждается руководством органа внутренних дел.

в) определить подход к оценке рисков органа внутренних дел, для чего необходимо:

- определить методологию оценки риска, подходящую для СУИБ, которая должна соответствовать требованиям обеспечения деятельности органа внутренних дел и нормативно-правовым требованиям информационной безопасности;

- разработать критерии принятия риска и определить приемлемые уровни риска.

Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты.

г) идентифицировать риски, для чего необходимо:

- идентифицировать активы в пределах области функционирования СУИБ и определить владельцев¹ этих активов.

- идентифицировать угрозы этим активам;

- идентифицировать уязвимости активов, которые могут быть использованы угрозами;

- идентифицировать последствия воздействия на активы в результате возможной утраты конфиденциальности, целостности и доступности активов;

д) проанализировать и оценить риски, для чего необходимо:

- оценить ущерб для деятельности органа внутренних дел, который может быть нанесен в результате сбоя обеспечения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

- оценить реальную вероятность сбоя обеспечения безопасности с учетом превалирующих угроз, уязвимостей и их последствий, связанных с этими активами, а также с учетом применяемых мер управления безопасностью;

- оценить уровни рисков;

- определить, являются ли риски приемлемыми или требуют обработки с использованием критериев допустимости рисков;

ж) определить и оценить различные варианты обработки рисков. Возможные действия:

- применение подходящих мер управления;

- сознательное и объективное принятие рисков при условии, что они полностью соответствуют требованиям политики и критериям органа внутренних дел в отношении принятия рисков;

- избежание рисков;

з) выбрать цели и меры управления для обработки рисков.

Цели и меры управления должны быть выбраны и реализованы так, чтобы удовлетворять требованиям, определенным в процессе оценки и обработки рисков. Этот выбор должен учиты-

¹ Здесь и далее «владелец» определяет лицо или организацию, которые имеют утвержденные руководством обязательства по контролю за производством, разработкой, поддержкой, использованием и безопасностью активов. Термин «владелец» не означает, что лицо действительно имеет какие-либо права собственности на актив.

вать критерии принятия рисков, а также нормативно-правовые требования и договорные обязательства.

и) получить утверждение руководством предполагаемых остаточных рисков;

к) получить разрешение руководства на внедрение и эксплуатацию СУИБ.

2.4.2. Внедрение и функционирование системы управления информационной безопасностью

Орган внутренних дел должен выполнить следующее:

а) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении управления рисками ИБ;

б) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

в) внедрить меры управления для достижения целей управления;

г) определить способ измерения результативности¹ выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные.

д) реализовать программы по обучению и повышению квалификации сотрудников;

е) управлять работой СУИБ;

ж) управлять ресурсами СУИБ;

з) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

¹ Измерение результативности мер управления позволяет руководителям и персоналу определить, в какой степени меры управления способствуют достижению намеченных целей управления.

2.4.3. Проведение мониторинга и анализа системы управления информационной безопасностью

Орган внутренних дел должен осуществлять следующее:

а) выполнять процедуры мониторинга и анализа, а также использовать другие меры управления в следующих целях:

- своевременно обнаруживать ошибки в результатах обработки;
- своевременно выявлять удавшиеся и неудавшиеся попытки нарушения и инциденты ИБ;
- предоставлять руководству информацию для принятия решений о ходе выполнения функций по обеспечению ИБ, осуществляемых как ответственными лицами, так и информационными технологиями;
- способствовать обнаружению событий ИБ и, таким образом, предотвращать инциденты ИБ путем применения средств индикации;
- определять, являются ли эффективными действия, принимаемые для устранения нарушения безопасности;

б) проводить регулярный анализ результативности СУИБ (включая проверку ее соответствия политике и целям СУИБ и анализ мер управления безопасностью) с учетом результатов аудиторских проверок ИБ, ее инцидентов, результатов измерений эффективности СУИБ, а также предложений и другой информации от всех заинтересованных сторон;

в) измерять результативность мер управления для проверки соответствия требованиям ИБ;

г) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения:

- в органе внутренних дел;
- в технологиях;
- в целях деятельности и процессах;
- в выявленных угрозах;
- в результативности реализованных мер управления;
- во внешних условиях, например изменения нормативно-правовых требований, требований договорных обязательств, а также изменения в социальной структуре общества;

д) проводить внутренние аудиты СУИБ через установленные периоды времени.

е) регулярно проводить руководством органа внутренних дел анализ СУИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;

ж) обновлять планы ИБ с учетом результатов анализа и мониторинга;

з) регистрировать действия и события, способные повлиять на результативность или функционирование СУИБ.

2.4.4. Поддержка и улучшение системы управления информационной безопасностью

Орган внутренних дел должен регулярно осуществлять следующее:

а) выявлять возможности улучшения СУИБ;

б) предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ИБ, полученный как в собственном органе внутренних дел, так и в других организациях;

в) передавать подробную информацию о действиях по улучшению СУИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;

г) обеспечивать внедрение улучшений СУИБ для достижения запланированных целей.

3. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основные варианты стратегии анализа рисков информационной безопасности органа внутренних дел

Прежде чем приступить к любым действиям, связанным с анализом риска, орган внутренних дел должен иметь стратегию проведения такого анализа, причем составные части этой стратегии (методы, способы и т. д.) должны быть отражены в содержании политики обеспечения безопасности информационных технологий. Эти методы и критерии выбора вариантов стратегии анализа риска должны отвечать потребностям органа внутренних дел. Стратегия анализа риска должна обеспечивать соответствие выбранного варианта стратегии условиям осуществления служебной деятельности и приложения усилий по обеспечению безопасности в тех областях, где это действительно необходимо. Рассматриваемые ниже варианты стратегии представляют собой четыре разных подхода к анализу риска. Основное различие между ними состоит в степени глубины проводимого анализа. Поскольку обычно проведение детального анализа риска для всех систем информационных технологий сопряжено со слишком большими затратами, тогда как поверхностное рассмотрение проблем, связанных с серьезным риском, не дает нужного эффекта, необходимо найти баланс между рассматриваемыми ниже вариантами.

Если не рассматривать вариант стратегии анализа риска, заключающийся в отсутствии принятия каких-либо защитных мер, и допустить, что реально появление различных видов риска неизвестного уровня и интенсивности, то существуют четыре основных варианта стратегии анализа рисков информационной безопасности органа внутренних дел:

- использование базового подхода (с низкой степенью риска) для всех систем информационных технологий, независимо от уровня риска, которому подвергаются системы, принятие того, что уровень обеспечения безопасности не всегда может оказаться достаточным;

- использование неформального подхода к проведению анализа риска, обращая особое внимание на системы информационных технологий, которые, как представляется, подвергаются наибольшему риску;

- проведение детального анализа риска с использованием формального подхода ко всем системам информационных технологий;

- проведение сначала анализа риска «высокого уровня» с тем, чтобы определить, какие из систем информационных технологий подвержены высокому уровню риска и какие имеют критическое значение для ведения деловых операций, с последующим проведением детального анализа риска для выделенных систем, а для всех остальных - ограничиваются применением базового подхода к проблемам обеспечения безопасности.

Ниже рассматриваются возможные варианты подхода к обеспечению безопасности и приводятся рекомендации по выбору предпочтительных вариантов.

Если орган внутренних дел решит не уделять внимания вопросам безопасности или отложить на потом внедрение защитных мер, то ее руководство должно ясно представлять себе возможные последствия такого решения. Хотя в этом случае отпадает необходимость затрат времени, средств, рабочих или других ресурсов, такое решение имеет ряд недостатков. Если орган внутренних дел не уверен в том, что функционирование его систем информационных технологий абсолютно не критично к внешним угрозам, он может впоследствии встретиться с серьезными проблемами. Так, орган внутренних дел может нарушить положения каких-либо законодательных и нормативных актов или репутация органа внутренних дел может пострадать в случае несанкционированных доступов к информации и неприятия действий по их предупреждению. Если орган внутренних дел не очень заботят проблемы обеспечения безопасности информационных технологий или он не имеет систем, безопасность которых важна для ведения служебной деятельности, он может следовать подобной стратегии. Однако, при этом не будет иметь представления о том, насколько хорошо или плохо реальное состояние его дел, так что для большинства организаций следование такой стратегии вряд ли является правильным.

3.1.1. Базовый подход

В случае использования первого варианта подхода к анализу риска орган внутренних дел может применить базовый уровень обеспечения безопасности ко всем системам информационных технологий путем выбора стандартных защитных мер безопасности. Перечень рекомендуемых стандартных защитных мер приведен в документах по базовой безопасности [19].

Существует ряд преимуществ использования этого варианта подхода, в том числе:

- возможность обойтись минимальным количеством ресурсов при проведении анализа и контроля риска для каждого случая принятия защитных мер и, соответственно, потратить меньше времени и усилий на выбор этих мер;

- при применении базовых защитных мер безопасности можно принять экономически эффективное решение, поскольку те же или схожие базовые защитные меры безопасности могут быть без особых проблем применены во многих системах, если большое число систем в рамках органа внутренних дел функционирует в одних и тех же условиях и предъявляемые к обеспечению безопасности требования соизмеримы.

В то же время этот вариант подхода имеет следующие недостатки:

- если принимается слишком высокий базовый уровень, то для ряда систем информационных технологий уровень обеспечения безопасности будет завышен;

- если базовый уровень будет принят слишком низким, то для ряда систем информационных технологий уровень обеспечения безопасности будет недостаточен, что увеличит риск ее нарушения и

- могут возникнуть трудности при внесении изменений, затрагивающих вопросы обеспечения безопасности. Так, если была проведена модернизация системы, то могут возникнуть сложности при оценке способностей первоначально примененных базовых защитных мер безопасности и далее оставаться достаточно эффективными.

Если все используемые в органе внутренних дел системы информационных технологий характеризуются низким уровнем

требований к обеспечению безопасности, то первый вариант стратегии анализа риска может оказаться экономически эффективным. В этом случае базовый уровень безопасности должен выбираться так, чтобы он соответствовал уровню защиты, необходимому для большинства систем информационных технологий. Для большинства организаций всегда существует необходимость использовать некоторые минимальные стандартные уровни для обеспечения защиты важнейшей информации с целью отвечать требованиям правовых и нормативных актов - например, требованиям нормативных правовых актов по безопасности информации. Однако в случаях, если отдельные системы органа внутренних дел характеризуются различной степенью чувствительности, разными объемами и сложностью служебной информации, использование общих стандартов применительно ко всем системам будет логически неверным, экономически неоправданным.

3.1.2. Неформальный подход

Второй вариант подхода предусматривает проведение неформального анализа риска, основанного на практическом опыте конкретного эксперта. Неформальный подход предполагает использование знаний и практического опыта специалистов, а не структурных методов.

Этот подход обладает следующими достоинствами:

- не требует использования значительных средств или времени. При его использовании эксперт не должен приобретать дополнительные знания по своей специальности, а затраты времени на анализ риска при этом меньше, чем при проведении детального анализа риска.

Однако данный подход имеет и свои недостатки:

- при отсутствии хотя бы одного элемента базового подхода (первый вариант стратегии анализа риска) или комплексного перечня контрольных операций увеличивается вероятность пропуска ряда важных деталей у всех систем информационных технологий, действующих в органе внутренних дел;

- могут возникнуть трудности при обосновании необходимости реализации защитных мер, определенных по результатам анализа риска, проведенного подобным подходом;

- для экспертов, не обладающих значительным опытом работы в области анализа рисков, не существует готовых рекомендаций, которые могли бы облегчить их работу;

- подходы органа внутренних дел к анализу риска в прошлом были продиктованы исключительно оценкой уязвимости систем, т. е. потребность в мерах обеспечения безопасности основывалась на наличии у этих систем уязвимостей без анализа того, существуют ли угрозы, способные реализовать наличие этих уязвимостей (без обоснования реальной необходимости в использовании защитных мер);

- результаты проведения анализа могут в какой-то мере зависеть от субъективного подхода, личных предубеждений эксперта и, кроме того, могут возникнуть проблемы в случае, если специалист, который проводил неформальный анализ, покидает организацию.

С учетом приведенных выше недостатков второй вариант подхода к анализу риска для многих организаций будет неэффективным.

3.1.3. Детальный анализ риска

Третий вариант подхода предполагает проведение детального анализа рисков с получением результатов для всех систем информационных технологий, действующих в органе внутренних дел. Детальный анализ рисков включает в себя подробную идентификацию и оценку активов, оценку возможных угроз, которым могут подвергнуться эти активы, а также оценку уровня их уязвимости. Результаты этих операций затем используют для оценки рисков и последующей идентификации обоснованных защитных мер.

Этот вариант подхода имеет следующие преимущества:

- весьма вероятно, что в результате этого подхода для каждой из систем будут определены соответствующие ей защитные меры обеспечения безопасности;

- результаты проведения детального анализа могут быть использованы при управлении изменениями в системе обеспечения безопасности.

В то же время такой вариант подхода характеризуется следующими недостатками:

- для его реализации и получения нужного результата требуется затратить значительное количество средств, времени и квалифицированного труда;

- существует вероятность того, что определение необходимых защитных мер для какой-либо критической системы произойдет слишком поздно, поскольку анализ будет проводиться одинаково тщательно для систем информационных технологий и для проведения анализа всех систем потребуется значительное время.

Таким образом, использование детального анализа риска применительно ко всем системам информационных технологий не рекомендуется. Если принято решение прибегнуть к такому варианту подхода, то возможны следующие дополнительные разновидности его использования:

- стандартный подход, отвечающий критериям настоящего стандарта;

- стандартный подход в разных вариантах, отвечающий потребностям органа внутренних дел.

3.1.4. Комбинированный подход

В соответствии с четвертым вариантом подхода предполагается проводить предварительный анализ высокого уровня риска для всех систем информационных технологий, обращая особое внимание на служебную значимость системы и уровень риска, которому она подвергается. Для систем информационных технологий, которые имеют важное значение для служебной деятельности органа внутренних дел и/или подвержены высокому уровню риска, в первую очередь проводят детальный анализ риска. Для остальных систем информационных технологий следует ограничиться базовым вариантом подхода. Таким образом, комбинированный вариант, сочетающий лучшие свойства подходов, описанных в 3.1 и 3.3, позволяет при сведении к минимуму времени и усилий, затраченных на идентификацию должных защитных мер, обеспечить необходимую защиту систем с высоким уровнем риска.

Кроме того, комбинированный вариант подхода имеет следующие преимущества:

- использование быстрого и простого предварительного анализа риска позволит обеспечить принятие программы анализа риска;

- существует возможность быстро оценить оперативное состояние программы обеспечения безопасности органа внутренних дел, т. е. использование такого подхода будет в значительной мере способствовать успешному планированию;

- ресурсы и средства могут быть вложены туда, где они принесут максимальный эффект, так как они в первую очередь будут направлены в системы, в наибольшей степени нуждающиеся в обеспечении безопасности;

- проведение последующих мероприятий будет более успешным.

Единственный потенциальный недостаток данного варианта подхода состоит в следующем: поскольку предварительный анализ риска проводят исходя из предположения о его возможном высоком уровне, отдельные системы могут быть ошибочно отнесены к системам, не требующим проведения детального анализа риска. К этим системам в дальнейшем будут применены базовые методы обеспечения безопасности. При необходимости можно будет вернуться к рассмотрению этих систем с тем, чтобы удостовериться, не требуют ли они более тщательного по сравнению с базовым подходом рассмотрения.

Использование данного варианта подхода с анализом высокого уровня риска в сочетании с базовым подходом и (если необходимо) детальным анализом риска обеспечивает большинству органов внутренних дел наиболее эффективное решение проблем. Таким образом, подобный подход является наиболее предпочтительным и будет более подробно рассмотрен далее в этом разделе.

3.1.4.1. Анализ высокого уровня риска

Прежде всего проводят предварительный анализ высокого уровня риска с тем, чтобы установить, какой из вариантов подхода (базовый или детальный) лучше подходит для конкретной системы информационных технологий. В ходе проведения такого предварительного анализа рассматривают служебную значимость систем информационных технологий и обрабатываемой с их по-

мощью информации, а также уровня риска с учетом вида служебной деятельности органа внутренних дел. Исходные данные для принятия решения о том, какой вариант подхода является наиболее подходящим для каждой системы информационных технологий, могут быть получены на основе рассмотрения следующих условий:

- служебных целей, для достижения которых орган внутренних дел использует данную систему информационных технологий;
- в какой степени оперативно-служебная деятельность органа внутренних дел зависит от конкретной системы информационных технологий, т. е. насколько функции, которые орган внутренних дел считает критическими для своего существования или эффективной реализации служебной деятельности, зависят от функционирования этой системы или обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации, обрабатываемой этой системой;
- вложения денежных средств в эту систему информационных технологий, в том числе в ее разработку, обслуживание или замену;
- активов данной системы ИТ, в которые орган внутренних дел вкладывает средства.

После того как эти условия проанализированы, принятие решения обычно не вызывает затруднений. Если целевое назначение системы важно для проведения органом внутренних дел своей служебной деятельности, если стоимость замены системы высока или средства, вложенные в активы, подвержены высокому уровню риска, то для данной системы необходимо проведение детального анализа риска. Наличие одного из перечисленных выше условий может служить основанием для проведения детального анализа риска.

Придерживаются следующего общего правила: если прекращение функционирования данной системы информационных технологий может причинить ущерб или принести убытки органу внутренних дел, отрицательно повлиять на его оперативно-служебную деятельность или активы, то для оценки потенциального риска проводят детальный анализ риска. Во всех других случаях достаточная безопасность системы может быть обеспечена применением базового подхода.

3.1.4.2. Применение базового подхода

Цель обеспечения безопасности с помощью базового подхода состоит в том, чтобы подобрать для органа внутренних дел минимальный набор защитных мер для защиты всех или отдельных систем информационных технологий. Используя базовый подход, можно применять соответствующий ему базовый уровень безопасности в органе внутренних дел и, кроме того, дополнительно использовать результаты детального анализа риска для обеспечения безопасности систем информационных технологий с высоким уровнем риска или систем, играющих важную роль в служебной деятельности органа внутренних дел. Использование базового подхода позволяет снизить инвестиции органа внутренних дел на исследование результатов анализа риска.

Удовлетворительная защита с помощью базового подхода может быть обеспечена путем использования справочных материалов (каталогов) по защитным мерам безопасности, где можно подобрать набор средств для защиты системы информационных технологий от наиболее часто встречающихся угроз. Базовый уровень безопасности может быть установлен в соответствии с потребностями органа внутренних дел, при этом в проведении детальной оценки угроз, рисков и уязвимости систем не будет необходимости. Все, что нужно сделать, применяя базовый подход к обеспечению безопасности, - выбрать из справочных материалов (каталогов) по защитным мерам безопасности соответствующие пункты, которые подходят для рассматриваемой системы информационных технологий. При наличии в системе установленных защитных мер их необходимо сравнить с рекомендуемыми в каталогах. Защитные меры, которые отсутствуют в системе, но могут быть в ней использованы, должны быть реализованы.

Справочные материалы (каталоги) по защитным мерам безопасности могут содержать во-первых, подробное описание рекомендуемых защитных мер, во-вторых, рекомендации с набором требований по обеспечению безопасности, которыми можно воспользоваться при выборе рекомендуемых мер для данной системы. Оба варианта имеют свои преимущества. Сведения о справочных материалах обоих вариантов можно найти в приложениях

А-Н, приведенных в ГОСТ Р ИСО/МЭК ТО 13335-4-2007 [19]. Одной из целей базового подхода является согласование защитных мер в масштабе всего органа внутренних дел, что может быть достигнуто при использовании каждого из указанных выше вариантов.

В настоящее время существует несколько справочников, содержащих перечни базовых защитных мер. После изучения их основных потребностей может оказаться, что справочники с перечнем базовых мер безопасности могут быть использованы несколькими различными органами внутренних дел. Такие справочники можно найти, например, в:

- международных организациях по стандартизации и национальных научно-технических центрах по стандартизации и метрологии;
- научно-технических центрах отраслевых стандартов (или нормативов);
- органах внутренних дел, имеющих аналогичную деловую деятельность или сопоставимых по масштабам работ.

Любой орган внутренних дел может выработать свой базовый уровень безопасности в соответствии с собственными условиями служебной деятельности и служебными целями.

3.1.4.3. Детальный анализ риска

Как было показано ранее детальный анализ риска для систем информационных технологий предполагает идентификацию всех возможных рисков и оценку их уровня. Необходимость проведения детального анализа риска может быть определена без ненужных затрат времени и средств после анализа высокого уровня риска для всех систем и последующего изучения результатов детального анализа риска, проведенного только для критических систем или систем с высоким уровнем риска.

Анализ риска проводится путем идентификации нежелательных событий, создающих неблагоприятные служебные ситуации, и определения вероятности их появления. Нежелательные события также могут негативно влиять на оперативно-служебную деятельность, сотрудников органа внутренних дел или любой элемент служебного процесса. Такое неблагоприятное воздей-

ствие нежелательных событий является сложным сочетанием возможных видов ущерба, наносимого активам, подвергающихся риску. Вероятность такого события зависит от того, насколько привлекательным является данный актив для потенциального нарушителя, вероятности реализации угроз и легкости, с какой нарушитель может воспользоваться уязвимыми местами системы. Результаты анализа риска позволяют идентифицировать системы информационных технологий с высоким уровнем риска и выбрать меры обеспечения безопасности, которые могут быть использованы для снижения уровня идентифицированного риска до приемлемого уровня.

3.2. Управление рисками информационной безопасности

Управление риском на основе детального анализа риска приведены на рисунке 2. Результаты детального анализа риска позволяют проводить выбор обоснованных защитных мер как части процесса управления риском. Требования, предъявляемые к выбранным мерам защиты, должны быть зафиксированы в политике безопасности систем информационных технологий и соответствующем ей плане безопасности. Множество инцидентов, связанных с нарушением системы безопасности, и внешние угрозы могут оказать влияние на требования к обеспечению безопасности системы и вызвать необходимость в пересмотре части анализа риска (или анализа в целом). К таким внешним угрозам могут относиться: недавние существенные изменения в системе, запланированные изменения, а также последствия инцидентов нарушений безопасности, по которым необходимо принимать соответствующие меры.

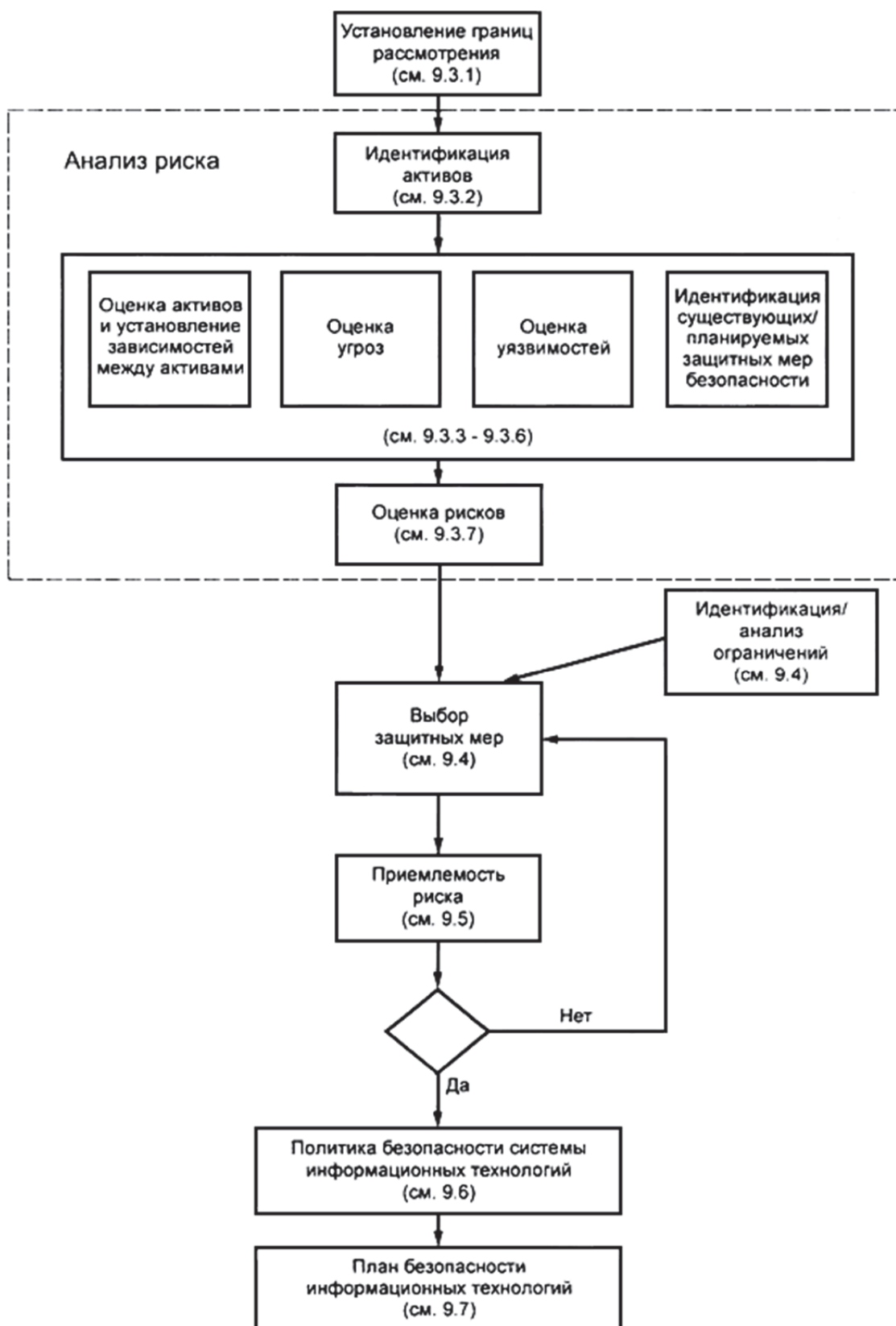


Рис. 2. Управление риском с использованием детального анализа риска

Существует несколько методов проведения анализа риска, начиная с подходов, основывающихся на перечне контрольных операций, и кончая методами, основанными на структурном анализе системы. При этом могут использоваться как автоматизированные (компьютерные) программы, так и расчет вручную. Любые метод или программа, используемые органом внутренних дел, должны, по меньшей мере, содержать операции, перечисленные в пунктах 3.2.1 – 3.2.7. Важно также, чтобы используемые методы не противоречили практике ведения дел, сложившейся в органе внутренних дел.

После завершения первого этапа рассмотрения результатов детального анализа рисков для системы результаты рассмотрения - сведения о активах и их ценностях, угрозах, уязвимостях и уровнях риска, определенных мерах обеспечения безопасности - должны быть сохранены (например в базе данных системы). Применение методов, использующих вспомогательные программные средства, сильно облегчает эту работу.

Представляемая информация, иногда рассматриваемая в качестве модели, может быть затем довольно эффективно использована после того как со временем с ней происходят изменения, не зависящие от конфигурации, типа обрабатываемой информации, сценариев угроз и т. д. При этом в качестве входных данных приводят только сведения об этих изменениях, что позволяет определить влияние изменений на необходимые меры обеспечения безопасности. Более того, такие модели могут быть использованы для быстрого изучения различных вариантов, например, при разработке новой системы информационных технологий или применительно к другим системам со схожими принципами построения.

3.2.1. Установление границ рассмотрения

Прежде чем получить исходные данные для идентификации и оценки активов, необходимо определить границы рассмотрения (см. рисунок 2). Тщательное определение границ на этой стадии анализа риска позволяет избежать ненужных операций и повысить качество анализа риска. Установление границ рассмотрения должно четко определить, какие из перечисленных ниже ресур-

сов должны быть учтены при рассмотрении результатов анализа риска. Для конкретной системы информационных технологий учитывают:

- активы информационных технологий (например, аппаратные средства, информационное обеспечение, информация);
- служащих (например, персонал органа внутренних дел, субподрядчики, персонал сторонних организаций);
- условия осуществления служебной деятельности (например, здания, оборудование);
- служебную деятельность (операции).

3.2.2. Идентификация активов

Актив системы информационных технологий является компонентом или частью общей системы, в которую орган внутренних дел напрямую вкладывает средства, и который, соответственно, требует защиты со стороны органа внутренних дел. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства и программное обеспечение. Могут существовать следующие типы активов:

- информация/данные (например, файлы, содержащие служебную информацию);
- аппаратные средства (например, компьютеры, принтеры);
- программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения);
- оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели);
- программно-аппаратные средства (например, гибкие магнитные диски, CD-ROM, программируемые ROM);
- документы (например, контракты);
- фонды (например, документы в архивах);
- оборудование, обеспечивающее необходимые условия работы;
- персонал органа внутренних дел;
- престиж (имидж) органа внутренних дел.

Активы, включенные в установленные границы рассмотрения, должны быть обнаружены, и наоборот, – любые активы, выведенные за границы рассмотрения (независимо от того, по каким соображениям это было сделано), должны быть рассмотрены еще раз с тем, чтобы убедиться, что они не были забыты или упущены.

3.2.3. Оценка активов и установление зависимости между активами

После того как все цели процесса идентификации активов были достигнуты и составлен перечень всех активов рассматриваемой системы информационных технологий, должна быть определена ценность этих активов. Ценность актива определяется его важностью для служебной деятельности органа внутренних дел, при этом уровень оценки служебной деятельности может исходить из соображений обеспечения безопасности, т. е. насколько может пострадать служебная деятельность органа внутренних дел и другие активы системы информационных технологий от утечки, искажения, недоступности и/или разрушения информации. Таким образом, идентификация и оценка активов, проведенные на основе учета служебных интересов органа внутренних дел, являются основным фактором в определении риска.

Исходные данные для оценки должны быть получены от владельцев и пользователей активов. Специалист(ы), проводящий(ие) анализ риска, должен(должны) составить перечень активов; при этом следует запросить содействие лиц, непосредственно занимающихся планированием служебной деятельности, финансами, информационными системами и другими соответствующими направлениями служебной активности для определения ценности каждого из активов. Полученные данные соотносят со стоимостью создания и обслуживания актива, а также с возможностью негативного воздействия на служебную деятельность, связанного с нарушением конфиденциальности, целостности, доступности, достоверности и надежности информации. Идентифицированные активы являются ценностью для органа внутренних дел. Однако невозможно непосредственно определить финансовую стоимость каждого из них. Необходимо также определить ценность или степень важности актива для органа внутренних

дел в служебной деятельности. В противном случае будет трудно определить уровень необходимой защиты и объем средств, которые органу внутренних дел следует израсходовать на принятие мер защиты. Примером шкалы оценок может быть деление уровня ценности как «низкий», «средний» или «высокий» или, с большей степенью детализации, «пренебрежимо малый», «низкий», «средний», «высокий», «очень высокий».

Независимо от используемой шкалы оценок, в ходе проведения оценки необходимо рассмотреть проблемы, связанные с уровнем возможного ущерба, причиной которого может быть:

- нарушение законодательства и/или технических норм;
- снижение уровня служебной активности;
- потеря/ухудшение репутации;
- нарушение конфиденциальности информации;
- возникновение угрозы личной безопасности;
- неблагоприятные последствия деятельности правоохранительных органов;
- нарушение общественного порядка;
- финансовые потери;
- перебои в выполнении служебных операций;

Каждый орган внутренних дел может выдвинуть также собственные критерии оценки, исходя из важности конкретных проблем для своей служебной деятельности. Кроме того, орган внутренних дел должен установить собственные границы для ущербов, определяемых как «низкие» и «высокие».

На этой стадии процесса оценки следует подчеркнуть, что метод оценки должен обеспечивать получение не только количественных, но и качественных оценок – там, где получение количественных оценок невозможно (например, возможность оценки стоимости потери жизни или служебной репутации). Используемая шкала оценок должна быть снабжена соответствующими пояснениями.

Следует также выявить виды зависимости одних активов от других, поскольку наличие таких видов зависимостей может оказать влияние на оценку активов. Например, конфиденциальность данных должна быть обеспечена на протяжении всего процесса их обработки, т. е. необходимость обеспечения безопасности программ обработки данных следует напрямую соотнести с

уровнем ценности конфиденциальности обрабатываемых данных. Кроме того, если служебная деятельность зависит от целостности вырабатываемых программой данных, то входные данные для этой программы должны иметь соответствующую степень надежности. Более того, целостность информации будет определяться качеством аппаратных средств и программного обеспечения, используемых для ее хранения и обработки. Функционирование аппаратных средств будет также зависеть от качества энергоснабжения и, возможно, от работы систем кондиционирования воздуха. Таким образом, данные о зависимостях, существующих между отдельными активами, будут способствовать идентификации некоторых видов угроз и определению конкретных уязвимостей, а использование данных о зависимостях даст уверенность в том, что активы оценены в соответствии с их реальной ценностью (с учетом существующих взаимозависимостей) и уровень безопасности выбран обоснованно.

Уровни ценности активов, от которых зависят другие активы, могут быть изменены в следующих случаях:

- если уровни ценности зависимых активов (например, данных) ниже или равны уровню ценности рассматриваемого актива (например, программного обеспечения), то этот уровень останется прежним;

- если уровни ценности зависимых активов (например, данных) выше, то уровень ценности рассматриваемого актива (например, программного обеспечения) необходимо повысить с учетом:

 - уровня соответствующей зависимости,
 - уровней ценности других активов.

Орган внутренних дел может иметь в своем распоряжении некоторые многократно используемые активы, например копии программ систем программного обеспечения или персональные компьютеры, подобные используемым в большинстве учреждений. Это необходимо учитывать при проведении оценки активов. С одной стороны, копии программ и т. д. в ходе оценки легко упустить из виду, и поэтому следует позаботиться о том, чтобы учесть их все; с другой стороны, их наличие может снизить остроту проблемы доступности информации.

Конечным результатом данного этапа является составление перечня активов и их оценка с учетом таких показателей, как раскрытие информации (сохранение конфиденциальности), изменение данных (сохранение целостности), невозможность доступа и разрушение информации (сокращение доступности) и стоимость замены.

3.2.4. Оценка угроз

Угроза (потенциальная возможность неблагоприятного воздействия) обладает способностью наносить ущерб системе информационных технологий и ее активам. Если эта угроза реализуется, она может взаимодействовать с системой и вызвать нежелательные инциденты, оказывающие неблагоприятное воздействие на систему. В основе угроз может лежать как природный, так и человеческий фактор; они могут реализовываться случайно или преднамеренно. Источники как случайных, так и преднамеренных угроз должны быть идентифицированы, а вероятность их реализации - оценена. Важно не упустить из виду ни одной возможной угрозы, так как в результате возможно нарушение функционирования или появление уязвимостей системы обеспечения безопасности информационных технологий.

Исходные данные для оценки угроз следует получать от владельцев или пользователей активов, специалистов по разработке оборудования и информационным технологиям, а также лиц, отвечающих за реализацию защитных мер в органе внутренних дел. Другие организации, например, федеральное правительство и местные органы власти, также могут оказать помощь при проведении оценки угроз, например, предоставить необходимые статистические данные. Полезным может быть использование перечня наиболее часто встречающихся угроз. Также полезно использование каталогов угроз (наиболее соответствующих нуждам конкретного органа внутренних дел или виду его служебной деятельности), так как ни один перечень не может быть достаточно полным. Ниже приведены некоторые наиболее часто встречающиеся варианты угроз:

- ошибки и упущения;
- мошенничество и кража;

- случаи вредительства со стороны персонала;
- ухудшение состояния материальной части и инфраструктуры;
- программное обеспечение хакеров, например имитация действий законного пользователя;
- программное обеспечение, нарушающее нормальную работу системы;
- промышленный шпионаж.

При использовании материалов каталогов угроз или результатов ранее проводившихся оценок угроз следует иметь в виду, что угрозы постоянно меняются, особенно в случае смены органом внутренних дел служебной направленности или информационных технологий. Нужно также отметить, что следствием внедрения таких мер защиты, как антивирусные программы, вероятно, является постоянное появление новых вирусов, не поддающихся воздействию действующих антивирусных программ.

После идентификации источника угроз (кто и что является причиной угрозы) и объекта угрозы (какой из элементов системы может подвергнуться воздействию угрозы) необходимо оценить вероятность реализации угрозы. При этом следует учитывать:

- частоту появления угрозы (как часто она может возникать согласно статистическим, опытным и другим данным), если имеются соответствующие статистические и другие материалы;
- мотивацию, возможности и ресурсы, необходимые потенциальному нарушителю и, возможно, имеющиеся в его распоряжении; степень привлекательности и уязвимости активов системы информационных технологий с точки зрения возможного нарушителя и источника умышленной угрозы;
- географические факторы – такие как наличие поблизости химических или нефтеперерабатывающих предприятий, возможность возникновения экстремальных погодных условий, а также факторов, которые могут вызвать ошибки у персонала, выход из строя оборудования и послужить причиной реализации случайной угрозы.

В зависимости от требуемой точности анализа может возникнуть необходимость разделить активы на отдельные компоненты и рассматривать угрозы относительно этих компонентов. Например, одним из таких активов можно считать актив, обозна-

ченный как «центральные серверы обслуживания данных», но если эти серверы расположены в различных географических точках, то этот актив необходимо разделить на «центральный сервер 1» и «центральный сервер 2», поскольку для серверов одни угрозы могут различаться по характеру опасности, а другие – по степени опасности. Таким образом, актив, включающий в себя программное обеспечение под объединенным названием «прикладное программное обеспечение», затем можно разбить на два или более элемента «прикладного программного обеспечения». Например, содержащий данные актив, вначале обозначенный как «досье на преступников», разбивают на два: «текст досье на преступников» и «изобразительная информация к досье на преступников».

После завершения оценки угроз составляют перечень идентифицированных угроз, активов или групп активов, подверженных этим угрозам, а также определяют степень вероятности реализации угроз с разбивкой на группы высокой, средней и низкой вероятности.

3.2.5. Оценка уязвимости

Этот вид оценки предполагает идентификацию уязвимостей окружающей среды, органа внутренних дел, процедур, персонала, управления, руководства, аппаратных средств, программного обеспечения или аппаратуры связи, которые могли бы быть использованы источником угроз для нанесения ущерба активам и служебной деятельности органа внутренних дел, осуществляемой с их использованием. Само по себе наличие уязвимостей не наносит ущерба, поскольку для этого необходимо наличие соответствующей угрозы. Наличие уязвимости при отсутствии такой угрозы не требует применения защитных мер, но уязвимость должна быть зафиксирована и в дальнейшем проверена на случай изменения ситуации. Следует отметить, что некорректно используемые, а также неправильно функционирующие защитные меры безопасности могут сами по себе стать источниками появления уязвимостей.

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива, которые могут использоваться иным образом

или для иных целей, чем те, для которых приобретался или изготавливался данный актив.

В процессе оценки уязвимости происходит идентификация уязвимостей, в которых могут быть реализованы возможные угрозы, а также оценка вероятного уровня слабости, т. е. легкости реализации угрозы. Например, отдельные виды активов можно легко продать, скрыть или переместить – эти их свойства могут быть связаны с наличием уязвимости. Исходные данные для оценки уязвимости должны быть получены от владельцев или пользователей актива, специалистов по обслуживающим устройствам, экспертов по программным и аппаратным средствам систем информационных технологий. Примерами уязвимостей могут быть:

- незащищенные подсоединения (например, к Интернету);
- неквалифицированные пользователи;
- неправильный выбор и использование пароля доступа;
- отсутствие должного контроля доступа (логического и/или физического);
- отсутствие резервных копий информационных данных или программного обеспечения;
- расположение ресурсов в районах, подверженных затоплению.

Важно оценить, насколько велика степень уязвимости или насколько легко ее можно использовать. Степень уязвимости следует оценивать по отношению к каждой угрозе, которая может использовать эту уязвимость в конкретной ситуации. Например, система может оказаться уязвимой к угрозе нелегального проникновения при идентификации пользователя и несанкционированного использования ресурсов. С одной стороны, степень уязвимости по отношению к нелегальному проникновению при идентификации пользователя может быть высокой в связи с отсутствием аутентификации пользователей. С другой стороны, степень уязвимости по отношению к несанкционированному использованию ресурсов может быть низкой, поскольку даже при отсутствии аутентификации пользователей способы несанкционированного использования ресурсов ограничены.

После завершения оценки уязвимостей должен быть составлен перечень уязвимостей и проведена оценка степени вероятности возможной реализации отмеченных уязвимостей, например «высокая», «средняя» или «низкая».

3.2.6. Идентификация существующих/планируемых защитных мер

Использование идентифицированных после рассмотрения результатов анализа риска защитных мер должно проводиться с учетом уже существующих или планируемых защитных мер. Действующие или планируемые защитные меры должны быть частью общего процесса, во избежание не вызываемых необходимостью затрат труда и средств, т. е. дублирования защитных мер. Кроме того, использование действующих или планируемых защитных мер может происходить без должного обоснования. В этом случае необходимо проверить, следует ли заменить меры обеспечения безопасности новыми, более обоснованными, или сохранить прежние (например, по экономическим соображениям).

Кроме того, необходимо провести дополнительную проверку с тем, чтобы определить, являются ли защитные меры безопасности, выбранные после проведения анализа риска, совместимыми с действующими и планируемыми мерами безопасности (т. е. выбранные и действующие меры безопасности не должны противоречить друг другу).

В процессе идентификации уже действующих защитных мер безопасности необходимо проверить, правильно ли они функционируют. Если предполагается, что какое-то средство защитной меры безопасности функционирует правильно, однако это не подтверждается в процессе осуществления деловых операций, то функционирование его может стать источником возможной уязвимости.

По результатам проведения идентификации защитных мер составляют перечень действующих и планируемых защитных мер безопасности с указанием статуса их реализации и использования.

3.2.7. Оценка рисков

Целью данного этапа является идентификация и оценка рисков, которым подвергаются рассматриваемая система информационных технологий и ее активы с тем, чтобы идентифицировать и выбрать подходящие и обоснованные защитные меры безопасности. Величина риска определяется ценностью подвергающихся

рisku активов, вероятностью реализации угроз, способных оказать негативное воздействие на деловую активность, возможностью использования уязвимостей идентифицированными угрозами, а также наличием действующих или планируемых защитных мер, использование которых могло бы снизить уровень риска.

Существуют различные способы учета таких факторов (активы, угрозы, уязвимости), например, можно объединить оценки риска, связанные с активами, уязвимостями и угрозами, для того чтобы получить оценки измерения общего уровня риска.

Вне зависимости от использованного способа оценки измерения риска результатом оценки прежде всего должно стать составление перечня оцененных рисков для каждого возможного случая раскрытия, изменения, ограничения доступности и разрушения информации в рассматриваемой системе информационных технологий. Составленный перечень оцененных рисков затем используют при идентификации рисков, на которые следует обращать внимание в первую очередь при выборе защитных мер. Метод оценки рисков должен быть повторяемым и прослеживаемым.

Как уже говорилось выше, для ускорения всех или отдельных элементов процесса анализа риска могут использоваться различные автоматизированные программные средства. Если орган внутренних дел решит использовать такие средства, необходимо проследить, чтобы выбранный подход соответствовал принятым в органе внутренних дел стратегии и политике безопасности информационных технологий. Кроме того, следует обратить особое внимание на правильность используемых входных данных, поскольку качество работы программных средств определяется качеством входных данных.

3.3. Выбор защитных мер

Для снижения оцененных уровней риска до приемлемых необходимо отобрать и идентифицировать подходящие и обоснованные меры безопасности. Для правильности выбора необходимо принять во внимание наличие действующих или запланированных мер безопасности, структуру обеспечения безопасности информационных технологий и наличие ограничений различного типа.

3.3.1. Определение защитных мер

Результаты оценки уровня риска, проведенной на предыдущем этапе, должны использоваться в качестве основы для идентификации защитных мер, необходимых для должного обеспечения безопасности системы.

Для выбора защитных мер, обеспечивающих эффективную защиту при некоторых уровнях риска, необходимо рассмотреть результаты анализа риска. Наличие уязвимости к определенным видам угроз позволяет определить, где и в какой форме необходимо использование дополнительных мер защиты.

Возможны также альтернативные варианты использования защитных мер, выбор которых производится исходя из стоимости рассмотренных защитных мер. Область использования защитных мер включает в себя:

- физическую окружающую среду;
- обслуживающий персонал;
- администрацию;
- аппаратные средства/программное обеспечение;
- средства обеспечения связи (коммуникации).

Действующие и запланированные меры защиты безопасности следует рассмотреть повторно с точки зрения их сравнительной стоимости (с учетом стоимости обслуживания) и принять решение об их невключении (или отказе от их реализации) или доработке, если они недостаточно эффективны. Следует отметить, что иногда удаление недостаточно эффективных действующих защитных мер обходится дороже, чем их использование и принятие дополнительных защитных мер (в случае необходимости). Возможны также случаи, когда действие защитных мер может быть распространено на активы, находящиеся вне установленных границ рассмотрения.

Для идентификации защитных мер полезно рассмотреть уязвимости системы, требующие защиты, и виды угроз, которые могут реализоваться при наличии этих уязвимостей. Существуют следующие возможности снижения уровня риска:

- избегать риска;
- уступить риск;
- снизить уровень угроз;

- снизить степень уязвимости системы ИТ;
- снизить возможность воздействия нежелательных событий;
- отслеживать появление нежелательных событий, реагировать на их появление и устранять их последствия.

Какая из этих возможностей (или их сочетание) окажется наиболее приемлемой для конкретного органа внутренних дел, зависит от конкретных обстоятельств. Существенную помощь может оказать также использование справочных материалов (каталогов) по защитным мерам безопасности. Однако при использовании защитных мер, выбранных по каталогу, необходимо их доработать с тем, чтобы они соответствовали специфическим требованиям органа внутренних дел.

Другим важным аспектом выбора защитных мер являются экономические соображения. Не следует рекомендовать использование защитных мер, стоимость реализации и эксплуатации которых превышала бы стоимость защищаемых активов. Также не рационально рекомендовать использование защитных мер, стоимость которых превышает бюджет того органа внутренних дел, где предполагается их использование. Однако следует с большой осторожностью подходить к случаям, когда из-за ограниченности бюджета приходится уменьшать число или снижать качество реализуемых защитных мер, поскольку это подразумевает возможность более высокого, чем планировалось, уровня риска. Принятый бюджет органа внутренних дел на защитные меры должен с осторожностью использоваться в качестве ограничивающего затраты фактора.

В случае, если для обеспечения безопасности системы информационных технологий используется базовый подход, выбор защитных мер сравнительно прост. Справочные материалы (каталоги) по защитным мерам безопасности предлагают набор защитных мер, способных защитить систему информационных технологий от наиболее часто встречающихся видов угроз. В этом случае рекомендуемые каталогом меры обеспечения безопасности следует сравнить с уже действующими или запланированными, а упомянутые в каталоге меры (отсутствующие или применение которых не планируется) должны составить перечень защитных мер, которые необходимо реализовать для обеспечения базового уровня безопасности.

Выбор защитных мер должен всегда включать в себя комбинацию организационных (не технических) и технических мер защиты. В качестве организационных рассматриваются меры, обеспечивающие физическую, персональную и административную безопасность.

Защитные меры для физической безопасности включают в себя обеспечение прочности внутренних стен зданий, использование кодовых дверных замков, систем пожаротушения и охранных служб. Обеспечение безопасности персонала включает в себя проверку лиц при приеме на работу (особенно лиц, нанимающихся на важные с точки зрения обеспечения безопасности должности), контроль за работой персонала и реализацию программ знания и понимания мер защиты.

Административная безопасность включает в себя безопасные способы ведения документации, наличие методов разработки и принятия прикладных программ, а также процедур обработки инцидентов в случаях нарушения систем безопасности. При таком способе обеспечения безопасности очень важно, чтобы для каждой системы была разработана система ведения служебной деятельности органа внутренних дел, предусматривающая в том числе возможность появления непредвиденных обстоятельств (ликвидацию последствий нарушения систем безопасности) и включающая в себя соответствующую стратегию и план (планы). План должен содержать подробные сведения о важнейших функциях и приоритетах, подлежащих восстановлению, необходимых условиях обработки информации и способах органа внутренних дел, которые необходимо осуществлять в случае аварии или временного прекращения работы системы. План должен содержать перечень шагов, которые следует предпринять для обеспечения безопасности важнейшей информации, подлежащей обработке, не прекращая при этом ведения организацией деловых операций.

Технические меры защиты предусматривают защиту аппаратных средств и программного обеспечения, а также систем связи. При этом выбор защитных мер проводят в соответствии с их степенью риска для обеспечения функциональной пригодности и надежной системы безопасности. Функциональная пригодность системы должна включать в себя, например, проведение идентификации и аутентификации пользователя, выполнение требова-

ний логического контроля допуска, обеспечение ведения контрольного журнала и регистрацию происходящих в системе безопасности событий, обеспечение безопасности путем обратного вызова запрашивающего, определение подлинности сообщений, шифрование информации и т. д. Требования к надежности систем безопасности определяют уровень доверия, необходимый при осуществлении функций безопасности, и тем самым определяют виды проверок, тестирования безопасности и т. д., обеспечивающих подтверждение этого уровня. При принятии решения об использовании дополнительного набора организационных и технических защитных мер могут быть выбраны разные варианты выполнения требований к обеспечению технической безопасности. Следует определить структуру технической безопасности для каждого из данных вариантов, с помощью которой можно получить дополнительное подтверждение правильности построения системы безопасности и возможности ее реализации на заданном технологическом уровне.

Орган внутренних дел может выбрать применение продукции и систем, прошедших оценку, в качестве одного из способов решения задачи окончательного построения системы безопасности. Продукцией и системой, прошедшими оценку, считаются те, испытания которых проводились третьей стороной. Этой третьей стороной может быть другое подразделение той же органа внутренних дел или независимая орган внутренних дел, специализирующаяся на оценке продукции и/или систем. Испытания могут проводиться на соответствие набору заранее установленных критериев оценки, которые формулируются, исходя из особенностей создаваемой системы; в тоже время может существовать обобщенный набор критериев оценки, соответствующих различным ситуациям. Критерии оценки продукции могут определять требования к функциональности и/или надежности продукции и систем.

В процессе выбора защитных мер, предлагаемых для реализации, необходимо учитывать ряд факторов, таких как:

- доступность использования защитных мер;
- прозрачность защитных мер для пользователя;
- в какой мере использование защитных мер помогает пользователю решать свои задачи;
- относительная надежность (стойкость) системы безопасности;

- виды выполняемых функций - предупреждение, сдерживание, обнаружение, восстановление, исправление, мониторинг и обмен информацией.

Обычно защитные меры предназначены для выполнения только некоторых из числа перечисленных выше функций (чем больше, тем лучше). При рассмотрении системы безопасности в целом или набора используемых защитных мер следует установить (если возможно) необходимые пропорции между видами функций, что позволит обеспечить большую эффективность и действенность системы обеспечения безопасности в целом. Может потребоваться проведение анализа рентабельности или анализа компромиссного решения (метод сравнения возможных альтернативных вариантов с использованием набора критериев, каждому из которых придается свое значение весового коэффициента в зависимости от его относительной важности применительно к определенной ситуации).

3.3.2. Структура безопасности информационных технологий

Структура безопасности информационных технологий отражает процесс обеспечения требований безопасности для отдельной системы информационных технологий как части общей структуры системы. Поэтому так важно рассмотрение структуры обеспечения безопасности информационных технологий в процессе выбора защитных мер.

Структура безопасности информационных технологий может использоваться при разработке новых систем, а также при внесении существенных изменений в существующие системы. Данная структура основывается на результатах анализа риска или базового подхода, должна учитывать требования к обеспечению безопасности и на их основе разработать набор технических мер защиты по обеспечению безопасности систем. В ряде случаев, если изменения вносят в существующие системы, некоторые требования могут быть в форме специфических защитных мер, которые должны быть использованы.

В структуре безопасности информационных технологий особое внимание уделяют техническим защитным мерам по обеспечению безопасности и достижению с их помощью целей

безопасности; при этом следует принимать во внимание также соответствующие нетехнические средства обеспечения безопасности. Хотя структура безопасности может быть построена на основе использования ряда различных подходов и перспектив, следует всегда учитывать следующий фундаментальный принцип ее построения: нельзя допускать неблагоприятное воздействие проблемы обеспечения безопасности в пределах уникальной зоны безопасности (зоны с одинаковыми или схожими требованиями к обеспечению безопасности и средствам ее защиты) на обеспечение безопасности в другой отдельной зоне безопасности. Структура безопасности информационных технологий обычно включает в себя одну или более зон безопасности. Зоны безопасности должны соответствовать областям служебной деятельности органа внутренних дел. Эти области служебной деятельности могут соответствовать функциональным секторам отдельных видов служебной деятельности органа внутренних дел, или они могут соответствовать функциональным секторам.

В зависимости от наличия одного или нескольких признаков существуют различные типы зон безопасности. Примерами признаков могут быть:

- уровни, категории или виды информации, доступные в пределах зоны безопасности;
- операции, которые могут проходить в пределах зоны безопасности;
- объединения по интересам, ассоциируемые с зоной безопасности;
- отношения к другим зонам безопасности и окружающим их средам;
- виды функций или доступ к информации, которые могут запрашивать объединения по интересам внутри зоны безопасности.

При построении структуры обеспечения безопасности информационных технологий необходимо также учитывать следующие проблемы:

- взаимоотношения и взаимозависимости между отдельными зонами безопасности;
- роль (или участие) взаимоотношений и взаимозависимостей в снижении качества услуг по обеспечению безопасности;

- необходимость органа внутренних дел дополнительных услуг или принятия дополнительных мер защиты для исправления, контроля или недопущения случаев снижения качества услуг.

Структура безопасности информационных технологий не существует сама по себе, но опирается на содержание других документов по информационным технологиям и согласовывается с ними. Наиболее важными из этих документов являются структура системы информационных технологий и структуры других соответствующих систем (аппаратные средства, средства связи и прикладные программы). Структура безопасности информационных технологий не должна содержать полного описания системы ИТ, а только описание технических вопросов и элементов, касающихся обеспечения безопасности. Назначение этой структуры состоит в том, чтобы свести к минимуму случаи неблагоприятного воздействия на пользователей, обеспечивая при этом оптимальную внутреннюю защиту инфраструктуры систем ИТ.

К структуре безопасности информационных технологий имеет отношение множество других документов или она может находиться в подчиненном положении по отношению к ним. К числу таких документов относятся:

- проект безопасности информационных технологий;
- рабочая концепция безопасности информационных технологий;
- план безопасности информационных технологий;
- политика безопасности системы информационных технологий;
- документы по сертификации и аккредитации системы информационных технологий (в случае необходимости).

3.3.3. Идентификация и анализ ограничений

На выбор мер защиты влияют многие ограничения. Эти ограничения необходимо принимать во внимание при разработке и реализации рекомендаций. К типичным ограничениям относят:

- ограничения по времени.

Может существовать множество видов ограничений по времени. Например, первый вид – защитная мера безопасности –

должен быть реализован в пределах периода времени, приемлемого для руководства органа внутренних дел. Второй вид ограничения по времени – реализация конкретной защитной меры безопасности в пределах жизненного срока соответствующей системы. Третьим видом ограничения по времени может быть длительность периода времени, необходимого руководству органа внутренних дел для принятия решения о том, стоит ли и дальше подвергать систему угрозам наличия конкретного риска;

- финансовые ограничения.

Стоимость реализации рекомендуемых мер защиты не должна превышать ценности активов, для безопасности которых они предназначены. Необходимо сделать все возможное, чтобы не выйти за пределы выделенных на эти цели ассигнований. Однако в ряде случаев достижение необходимого уровня безопасности и приемлемого уровня риска может оказаться невозможным в пределах подобных финансовых ограничений. В этом случае выход из сложившейся ситуации предоставляется на усмотрение руководства органа внутренних дел;

- технические ограничения.

Технические проблемы, например, совместимость программ или аппаратных средств, легко разрешаются, если уделить им серьезное внимание в процессе выбора средств защиты. Кроме того, при реализации разработанных ранее защитных мер применительно к существующим системам часто возникают затруднения, связанные с техническими ограничениями. Наличие подобных затруднений могут переместить направленность (пересмотр выбора) защитных мер в сторону организационных и физических способов защиты;

- социологические ограничения.

Особенности социологических ограничений при выборе защитных мер могут зависеть от того, о какой стране, отрасли, органа внутренних дел или даже отделе органа внутренних дел идет речь. Этими ограничениями нельзя пренебрегать, поскольку эффективность использования многих технических защитных мер зависит от активной поддержки их сотрудниками органа внутренних дел. Если сотрудники не понимают необходимости таких мер или не считают их приемлемыми по моральным сооб-

ражениям, то существует большая вероятность того, что со временем эффективность защитных мер будет снижаться;

- ограничения окружающей среды.

На выбор защитных мер могут влиять также и экологические факторы, например, прилегающие территории, экстремальные природные условия, состояние окружающей среды и прилегающих городских территорий и т. д.;

- правовые ограничения.

Правовые ограничения, например, установленные законодательством требования о защите личной информации или статьи уголовного кодекса, касающиеся обработки информации, могут повлиять на выбор мер защиты. Законы и нормативы, не имеющие прямого отношения к защите информационных технологий, например, требования противопожарной безопасности и статьи трудового законодательства, могут также повлиять на выбор мер защиты.

3.4. Приемлемость рисков

После выбора защитных мер и идентификации снижения уровня риска в результате применения защитных мер всегда будут иметь место остаточные риски, поскольку система не может быть абсолютно безопасной. Эти остаточные риски должны оцениваться организацией как приемлемые или неприемлемые. Такая оценка может быть осуществлена путем рассмотрения потенциальных неблагоприятных воздействий на сферу служебной деятельности, которые могут быть вызваны остаточными рисками. Очевидно, что существование неприемлемых рисков нельзя допускать без дальнейшего их обсуждения. Необходимо управленческое решение о допустимости таких рисков в связи с имеющимися ограничениями (например, по затратам средств или невозможности предупреждения рисков - падение самолетов на здания или землетрясения; тем не менее планы восстановительных работ на случай подобных катастроф могут быть подготовлены) либо необходимо предусмотреть дополнительные и, возможно, дорогостоящие меры защиты для снижения уровня неприемлемых рисков.

4. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ АКТИВАМИ

4.1. Ответственность за активы

Цель: Обеспечить соответствующую защиту активов органа внутренних дел.

Все активы должны учитываться и иметь назначенного владельца.

Необходимо определять владельцев всех активов, и следует определять ответственного за поддержку соответствующих мер и средств контроля и управления. Реализация определенных мер и средств контроля и управления при необходимости может быть делегирована владельцем, но владелец остается ответственным за надлежащую защиту активов.

4.1.1. Инвентаризация активов

Все активы должны быть четко определены, должна составляться и поддерживаться опись всех важных активов.

Органу внутренних дел следует идентифицировать все активы и документально оформлять значимость этих активов. В опись активов следует включить всю информацию, необходимую для восстановления после бедствия, в том числе тип актива, формат, местоположение, информацию о резервных копиях, информацию о лицензировании и ценности для служебной деятельности. Опись не должна без необходимости дублировать другие описи, но следует обеспечивать уверенность в том, что ее содержание выверено.

Кроме того, владение и классификация информации должны быть согласованы и документально оформлены в отношении каждого актива. Основываясь на важности актива, его ценности для служебной деятельности и его степени секретности, надлежит определить уровни защиты, соответствующие значимости активов (более подробную информацию о том, как оценивать активы, чтобы учесть их важность, можно найти в ГОСТ Р ИСО/МЭК 27005-2010 [6]).

Существует много типов активов, включающих:

а) информацию: базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности служебной деятельности, меры по переходу на аварийный режим, контрольные записи и архивированная информация;

б) программные активы: прикладные программные средства, системные программные средства, средства разработки и утилиты;

в) физические активы: компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;

г) услуги: вычислительные услуги и услуги связи, основные поддерживающие услуги, например отопление, освещение, электроэнергия и кондиционирование воздуха;

д) персонал, его квалификация, навыки и опыт;

е) нематериальные ценности, например репутация и имидж органа внутренних дел.

Описи активов помогают обеспечивать уверенность в том, что активы органа внутренних дел эффективно защищены, данные описи могут также потребоваться для других целей, таких как обеспечение безопасности труда, страховые или финансовые (управление активами) вопросы. Процесс инвентаризации активов - важное условие для управления рисками информационной безопасности.

4.1.2. Владение активами

Вся информация и активы, связанные со средствами обработки информации должны находиться во владении.

Термином «владелец» определяется физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью активов. Термин «владелец» не означает, что данный человек фактически имеет право собственности на этот актив.

Владелец актива должен нести ответственность за:

а) обеспечение уверенности в том, что информация и активы, связанные со средствами обработки информации, классифицированы соответствующим образом;

б) определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом.

Владение может распространяться на:

а) процесс служебной деятельности;

б) определенный набор направлений деятельности;

в) прикладные программы;

г) определенное множество данных.

Повседневные задачи могут быть переданы, например должностному лицу, ежедневно работающему с активом, но ответственность сохраняется за владельцем.

В сложных информационных системах рекомендуется обозначить группы активов, действующих вместе, для обеспечения определенной функции, такой как «услуга». В данном случае владелец услуг является ответственным за поставку услуги и функционирование активов, которые обеспечивают данную услугу.



4.1.3. Приемлемое использование активов

Следует определять, документально оформлять и реализовывать правила приемлемого использования информации и активов, связанных со средствами обработки информации.

Всем сотрудникам, подрядчикам и представителям третьей стороны рекомендуется следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая:

а) правила использования электронной почты и Интернета;

б) рекомендации по использованию мобильных устройств.

Соответствующему управленческому персоналу должны быть предоставлены конкретные правила или рекомендации. Сотрудники, подрядчики и представители третьей стороны, использующие или имеющие доступ к активам органа внутренних дел, должны быть осведомлены о существующих ограничениях в

отношении использования ими информации и активов органа внутренних дел, связанных со средствами обработки информации и ресурсами. Они должны нести ответственность за использование ими любых средств обработки информации, и любое использование таких средств осуществлять под свою ответственность.

4.2. Классификация информации

Цель: Обеспечить уверенность в защищенности информации на надлежащем уровне.

Информацию следует классифицировать, чтобы определить необходимость, приоритеты и предполагаемую степень защиты при обработке информации.

Информация имеет различные степени чувствительности и критичности. Некоторые элементы могут потребовать дополнительного уровня защиты или специальной обработки. Схему классификации информации следует использовать для определения соответствующего множества уровней защиты и установления потребности в принятии специальных мер обработки.

4.2.1. Рекомендации по классификации

Информацию следует классифицировать, исходя из ее ценности, законодательных требований, чувствительности и критичности для органа внутренних дел.

При классификации информации и связанных с ней защитных мер и средств контроля и управления необходимо учитывать требования служебной деятельности в отношении совместного использования или ограничения доступа к информации и последствия для служебной деятельности, связанные с такими требованиями.

Рекомендации по классификации должны включать руководящие указания по начальной классификации и последующей классификации по истечении времени в соответствии с некой predetermined политикой управления доступом.

В обязанности владельца актива входит классификация актива, ее периодический пересмотр и обеспечение уверенности в том, что она поддерживается на актуальном и соответствующем

уровне. В отношении классификации следует учитывать эффект накопления.

Предметом рассмотрения должно стать количество классификационных категорий и преимущества, получаемые от их использования. Чрезмерно сложные схемы могут стать обременительными и неоправданно дорогими для применения, или могут оказаться неосуществимыми. Следует проявлять осторожность в интерпретации классификационных меток на документах из других организаций, так как одни и те же метки могут иметь различный смысл.

Уровень защиты может оцениваться с помощью анализа конфиденциальности, целостности и доступности, а также каких-либо других требований в отношении рассматриваемой информации.

Информация часто перестает быть чувствительной или критической по истечении некоторого периода времени, например, когда она делается общедоступной. Эти аспекты необходимо принимать во внимание, поскольку присвоение более высокой категории может привести к реализации ненужных мер и средств контроля и управления и, как следствие, к дополнительным расходам.

При назначении классификационных уровней, совместное рассмотрение документов с аналогичными требованиями безопасности может упростить задачу по классификации.

В общем, классификация информации - кратчайший путь для определения способа ее обработки и защиты.

4.2.2. Маркировка и обработка информации

Соответствующий набор процедур маркировки и обработки информации следует разрабатывать и реализовывать в соответствии с системой классификации, принятой органом внутренних дел.

Необходимо, чтобы процедуры маркировки информации охватывали информационные активы, представленные как в физической, так и в электронной форме.

Выводимые из систем документы, содержащие информацию, которая классифицирована как чувствительная или критическая, должны содержать соответствующий маркировочный знак. Маркированными могут быть напечатанные отчеты, экранные отображения, носители информации (например ленты, диски, компакт-диски), электронные сообщения и пересылаемые файлы.

Для каждого уровня классификации должны быть определены процедуры обработки, включающие безопасную обработку, хранение, передачу, снятие грифа секретности и уничтожение. Сюда следует также отнести процедуры по обеспечению сохранности и регистрации любого события, имеющего значение для безопасности.

Договоры с другими организациями, включающие требования о совместном использовании информации, должны содержать процедуры определения классификации этой информации и интерпретации классификационных меток других организаций.

Маркировка и безопасная обработка классифицированной информации является ключевым требованием для соглашений о совместном использовании информации. Физические метки являются наиболее распространенной формой маркировки. Однако некоторые информационные активы, например документы в электронной форме, не могут быть маркированы физически, и поэтому необходимо использовать электронные аналоги маркировки. Например, на экране или дисплее может появиться уведомляющая метка. Там, где маркировка неосуществима, применяют другие средства обозначения классификации информации, например с помощью процедур или метаданных.



5. УПРАВЛЕНИЕ ПЕРСОНАЛОМ

5.1. Перед трудоустройством

Под словом «трудоустройство» здесь понимается охват всех следующих отличающихся друг от друга ситуаций: трудоустройство людей (временное или постоянное), указание должностных функций (ролей), изменение должностных функций, определение срока действия договоров и прекращение любой из этих договоренностей.

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осознают свои обязанности и способны выполнять предусмотренные для них роли, и снизить риск хищения, мошенничества или нецелевого использования средств обработки информации.

Обязанности, связанные с обеспечением безопасности, следует оговаривать перед трудоустройством в соответствующих должностных инструкциях и условиями работы.

Необходима соответствующая проверка всех кандидатов на должность, подрядчиков и представителей третьей стороны, особенно если работа связана со сведениями, составляющими государственную тайну.

Сотрудники, подрядчики и представители третьей стороны, использующие средства обработки информации органа внутренних дел, должны подписывать соглашение в отношении их ролей и обязанностей в области безопасности.

5.1.1. Роли и обязанности

Роли и обязанности в области безопасности сотрудников, подрядчиков и представителей третьей стороны необходимо определять и оформлять документально в соответствии с политикой информационной безопасности органа внутренних дел.

Роли и обязанности в области безопасности должны включать в себя требования в отношении:

а) реализации и действия в соответствии с политиками информационной безопасности органа внутренних дел;

б) защиты активов от несанкционированного доступа, разглашения сведений, модификации, разрушений или вмешательства;
в) выполнения определенных процессов или деятельности, связанных с безопасностью;

г) обеспечения уверенности в том, что на индивидуума возлагается ответственность за предпринимаемые действия;

д) информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для органа внутренних дел.

Роли и обязанности в области безопасности должны быть определены и доведены до претендентов на работу до их трудоустройства.

Для документального оформления ролей и обязанностей в области безопасности могут использоваться должностные инструкции. Роли и обязанности в области безопасности лиц, поступивших на работу не через процесс трудоустройства, принятый в органе внутренних дел, а, например, с помощью сторонней организации должны быть также четко определены и доведены до сведения.



5.1.2. Предварительная проверка

Тщательная проверка всех кандидатов на постоянную работу (службу), подрядчиков и представителей третьей стороны должна проводиться согласно соответствующим законам, инструкциям и правилам этики, пропорционально требованиям служебной деятельности, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам.

При проверке следует учитывать конфиденциальность, защиту персональных данных и (или) трудовое законодательство. Такая проверка должна включать следующие элементы:

а) наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;

б) проверку (на предмет полноты и точности) биографии претендента;

в) подтверждение заявленного образования и профессиональной квалификации;

- г) независимую проверку подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);
- д) более детальную проверку, например кредитоспособности или на наличие судимости.

В случаях, когда новому сотруднику непосредственно после приема на работу или в дальнейшем предоставляется доступ к средствам обработки информации, в частности, обрабатывающим чувствительную информацию, например финансовую или секретную информацию, органа внутренних дел следует проводить дополнительную, более детальную проверку.

Процедуры должны определять критерии и ограничения процесса проверки, например кто имеет право проводить проверку сотрудников, каким образом, когда и с какой целью проводится эта проверка.

Предварительную проверку также следует проводить для подрядчиков и представителей третьей стороны. Как бы то ни было, в договорах с третьей стороной должны четко определяться все обязанности и процедуры уведомления, необходимые для предварительной проверки.

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в органе внутренних дел, следует собирать и обрабатывать согласно законодательству, действующему в соответствующей юрисдикции. В зависимости от действующего законодательства, данные кандидаты должны быть предварительно проинформированы о деятельности, связанной с предварительной проверкой.

5.1.3. Условия занятости

В рамках своих договорных обязательств, сотрудники, подрядчики и представители третьей стороны должны согласовать и подписать условия своего трудового договора, устанавливающего их ответственность и ответственность органа внутренних дел в отношении информационной безопасности.

Условия занятости должны отражать политику безопасности органа внутренних дел и, кроме того, разъяснять и констатировать:

а) что все сотрудники, подрядчики и представители третьей стороны, имеющие доступ к чувствительной информации, должны подписывать соглашение о конфиденциальности или неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации;

б) правовую ответственность и права сотрудников, подрядчиков и любых других лиц, например, в части законов об авторском праве или законодательства о защите персональных данных;

в) обязанности в отношении классификации информации и управления активами органа внутренних дел, связанных с информационными системами и услугами, выполняются сотрудником, подрядчиком или представителем третьей стороны;

г) ответственность сотрудника, подрядчика или представителя третьей стороны за обработку информации, получаемой от других лиц и/или сторонних организаций;

д) ответственность органа внутренних дел за обработку персональной информации, включая персональную информацию, полученную в результате или в процессе служебной деятельности органа внутренних дел;

е) ответственность, распространяющуюся также и на деятельность вне помещений органа внутренних дел и в нерабочее время;

ж) действия, которые должны быть предприняты в случае, если сотрудник, подрядчик или представитель третьей стороны игнорирует требования информационной безопасности органа внутренних дел.

Орган внутренних дел должен обеспечивать уверенность в том, что сотрудники, подрядчики и представители третьей стороны согласны с условиями, касающимися информационной безопасности и соответствующими типу и объему доступа, который они будут иметь к активам органа внутренних дел, связанным с информационными системами и услугами.

При необходимости ответственность, возлагаемая на сотрудника по условиям занятости, должна сохраняться сотрудником в течение определенного периода времени и после окончания работы в органе внутренних дел.

Может быть использован кодекс поведения для распространения информации, касающейся обязанностей сотрудников, подрядчиков или представителей третьей стороны в отношении конфиденциальности, защиты информации, правил этики, соответствующего использования оборудования и средств органа внутренних дел, а также порядка деятельности. Подрядчик или представители третьей стороны могут быть связаны со сторонней организацией, с которой, в свою очередь, может потребоваться заключить договорные соглашения от имени лица, подписавшего договор.



5.2. В течение занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, а также оснащены всем необходимым для поддержки политики безопасности органа внутренних дел, что снижает риск человеческого фактора.

Следует определять обязанности руководства, чтобы обеспечить уверенность в том, что безопасность обеспечивается на протяжении всего времени занятости сотрудника в органе внутренних дел.

Адекватный уровень осведомленности, обучения и тренинг процедурам безопасности и правильному использованию средств обработки информации должен быть обеспечен всем сотрудникам, подрядчикам и представителям третьей стороны, чтобы свести к минимуму возможные риски безопасности. Должен быть установлен формальный дисциплинарный процесс для рассмотрения нарушений безопасности.

5.2.1. Обязанности руководства

Руководство органа внутренних дел должно требовать, чтобы сотрудники, подрядчики и представители третьей стороны обеспечивали безопасность в соответствии с установленными политиками и процедурами органа внутренних дел.

Руководство обязано обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны:

а) были проинформированы о своих ролях и обязанностях в области информационной безопасности прежде, чем им был предоставлен доступ к чувствительной информации или информационным системам;

б) обеспечены рекомендациями по формулированию их предполагаемых ролей в отношении безопасности в рамках органа внутренних дел;

в) заинтересованы следовать политикам безопасности органа внутренних дел;

г) достигают уровня осведомленности в отношении безопасности, соответствующего их ролям и обязанностям в органе внутренних дел;

д) следуют условиям занятости, которые включают политику информационной безопасности органа внутренних дел и соответствующие методы работы;

е) продолжают поддерживать соответствующие навыки и квалификацию.

Дополнительная информация:

Если сотрудники, подрядчики и представители третьей стороны не были осведомлены о своих обязанностях в отношении безопасности, они могут причинить значительный ущерб органу внутренних дел. Заинтересованный персонал, вероятно, будет более надежным и вызовет меньше инцидентов информационной безопасности.

Неэффективное управление может являться причиной того, что персонал будет чувствовать себя недооцененным, что в дальнейшем может иметь негативные последствия для органа внутренних дел. Например, неэффективное управление может привести к игнорированию безопасности или возможному нецелевому использованию активов органа внутренних дел.



5.2.2. Осведомленность, обучение и тренинг в области информационной безопасности

Все сотрудники органа внутренних дел и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в органа внутренних дел и необходимых для выполнения их рабочих функций.

Обучение, обеспечивающее осведомленность, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями органа внутренних дел в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Постоянное обучение должно охватывать требования безопасности, правовую ответственность, управление служебной деятельностью, а также обучение правильному использованию средств обработки информации, например процедуре начала сеанса, использованию пакетов программ и информации о дисциплинарном процессе.

Деятельность, связанная с обеспечением осведомленности, обучения и тренинга в отношении безопасности должна быть адекватной и соответствовать роли, обязанностям и квалификации лица, и должна включать информацию об известных угрозах, о контактном лице для получения дополнительной консультации по безопасности, а также о соответствующих каналах для сообщения об инцидентах информационной безопасности.

Обучение с целью повышения осведомленности направлено на то, чтобы дать возможность отдельным лицам распознавать проблемы и инциденты информационной безопасности, и реагировать в соответствии с потребностями их рабочей функции.



5.2.3. Дисциплинарный процесс

Должен существовать формальный дисциплинарный процесс, применяемый в отношении сотрудников, совершивших нарушение безопасности.

Не следует начинать дисциплинарный процесс, не получив предварительного подтверждения того, что нарушение безопасности произошло.

Формальный дисциплинарный процесс призван обеспечить уверенность в корректном и справедливом рассмотрении дел сотрудников, подозреваемых в совершении нарушений безопасности. Формальный дисциплинарный процесс следует обеспечивать для дифференцированного реагирования, учитывающего такие факторы, как тип и тяжесть нарушения и его негативное влияние на оперативно-служебную деятельность, совершено ли нарушение впервые или повторно, получил ли нарушитель должную подготовку, соответствующее законодательство, договоры в сфере служебной деятельности и другие факторы, если в этом есть необходимость. В серьезных случаях неправомерного поведения процесс должен обеспечивать возможность безотлагательного аннулирования обязанностей, прав доступа и привилегий сотрудника и, при необходимости, немедленного удаления его из информационного процесса.

Дисциплинарный процесс следует также использовать как сдерживающее средство для предотвращения совершения сотрудниками, подрядчиками и представителями третьей стороны нарушений политик и процедур безопасности, принятых в органе внутренних дел, и каких-либо других нарушений безопасности.



5.3. Прекращение или смена занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны покидают организацию или меняют занятость должным образом.

Руководство органа внутренних дел обязано обеспечить уверенность в том, что при увольнении сотрудников, подрядчиков и представителей третьей стороны из органа внутренних дел,

осуществляется возврат всего оборудования, а также выполняется аннулирование всех прав доступа.

Изменения обязанностей и занятости, равно как и прекращение соответствующей обязанности и занятости в рамках органа внутренних дел должно управляться в соответствии с данным подразделом, а любая новая занятость должна управляться.

5.3.1. Прекращение обязанностей

Обязанности в отношении прекращения занятости или смены занятости должны быть четко определены и установлены.

Информирование о прекращении обязанностей должно включать в себя актуальные требования безопасности и правовую ответственность, и, при необходимости, обязанности, содержащиеся в соглашении о конфиденциальности, а также условия занятости, продолжающие действовать в течение определенного периода времени после прекращения занятости сотрудников, подрядчиков или представителей третьей стороны.

Ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, должны содержаться в договорах с сотрудниками, подрядчиками или представителями третьей стороны.

Изменения обязанности и занятости должны управляться так же, как и прекращение соответствующей обязанности или занятости.

Отдел кадров, как правило, отвечает за общий процесс прекращения занятости и действует совместно с руководителем увольняемого лица, чтобы обеспечить управление аспектами безопасности значимых процедур. В отношении подрядчика данный процесс может быть осуществлен подразделением, несущим ответственность за подрядчика, а в отношении представителя третьей стороны – его организацией.

Сотрудников, подрядчиков или представителей третьей стороны необходимо информировать об изменениях кадрового состава и действующих договоренностей



5.3.2. Возврат активов

Все сотрудники, подрядчики и представители третьей стороны обязаны вернуть органу внутренних дел все активы, находящиеся в их пользовании, при прекращении их занятости, договора или соглашения.

Процесс прекращения занятости должен быть формализован таким образом, чтобы включать в себя возврат всего ранее выданного программного обеспечения, корпоративных документов и оборудования. Необходимо возвращать также другие активы органа внутренних дел, например мобильную вычислительную технику, карты доступа, программное обеспечение, руководства и информацию, хранящуюся на электронных носителях.

В тех случаях, когда сотрудник, подрядчик или представитель третьей стороны покупает оборудование органа внутренних дел или использует свое собственное оборудование, необходимо следовать процедурам, обеспечивающим уверенность в том, что вся значимая информация была передана органу внутренних дел и удалена из оборудования безопасным образом.

В случаях, когда сотрудник, подрядчик или представитель третьей стороны располагает знаниями, важными для продолжающихся работ, такую информацию следует оформлять документально и передавать органу внутренних дел.

5.3.3. Аннулирование прав доступа

Права доступа всех служащих, подрядчиков и представителей третьей стороны к информации и средствам обработки информации должны быть аннулированы при прекращении занятости, договора или соглашения, или скорректированы при смене занятости.

При прекращении занятости, права доступа к активам, связанным с информационными системами, и услугам необходимо пересматривать. Это позволит определять, нужно ли аннулировать права доступа. Смена занятости должна сопровождаться аннулированием всех прав доступа, которые не санкционированы для новой занятости. Права доступа, которые должны быть аннулированы или адаптированы, касаются физического и логическо-

го доступа, ключей, идентификационных карт, средств обработки информации, подписок и удаления из любой документации, в которой они идентифицируются как фактические сотрудники органа внутренних дел. Если увольняемый сотрудник, подрядчик или представитель третьей стороны знал пароли к учетным записям, остающимся активными, то эти пароли должны быть изменены после прекращения занятости, договора или соглашения, или при смене занятости.

Права доступа к информационным активам и средствам обработки информации следует уменьшать или аннулировать до прекращения занятости или смены места занятости, в зависимости от оценки факторов риска, например:

а) было ли прекращение занятости или смена места занятости инициированы сотрудником, подрядчиком или представителем третьей стороны, или руководством, и причина прекращения занятости;

б) текущие обязанности сотрудника, подрядчика или любого другого представителя;

в) значимость активов, доступных в настоящий момент.

При определенных обстоятельствах права доступа могут распределяться на основе доступности для большего количества людей, чем только для увольняемого сотрудника, подрядчика или представителя третьей стороны, например групповые идентификаторы. При таких обстоятельствах увольняемых лиц следует исключать из любых списков группового доступа, и следует предпринимать меры, рекомендуемые всем другим связанным с доступом сотрудникам, подрядчикам и представителям третьей стороны не осуществлять совместно с увольняемым лицом использования этой информации.

В случаях, когда прекращение занятости инициируется руководством, рассерженные сотрудники, подрядчики или представители третьей стороны могут преднамеренно разрушать информацию или повреждать средства обработки информации. В случаях ухода в отставку, некоторые лица склонны собирать информацию для будущего использования.



6. УПРАВЛЕНИЕ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

6.1. Зоны безопасности

Цель: Предотвращать неавторизованный физический доступ, повреждение и воздействие в отношении помещений и информации органа внутренних дел.

Средства обработки критической или чувствительной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами, контролирующими вход. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен выявленным рискам.

6.1.1. Периметр зоны безопасности

Для защиты зон, которые содержат информацию и средства обработки информации, следует использовать периметры безопасности (барьеры, например стены, управляемые картами доступа ворота или турникеты, управляемые человеком).

В отношении физических периметров безопасности рекомендуется рассматривать и реализовывать, при необходимости, следующие рекомендации:

а) периметры безопасности должны быть четко определены, а размещение и надежность каждого из периметров должны зависеть от требований безопасности активов, находящихся в пределах периметра, и от результатов оценки риска;

б) периметры здания или помещений, где расположены средства обработки информации, должны быть физически прочными (т. е. не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть); внешние стены помещений должны иметь твердую конструкцию, а все внешние двери должны быть соответствующим образом защищены от неавторизованного доступа, например оснащены шлагбаумом, сигнализацией, замками т.п.; двери и окна помещений в отсутствие сотрудников должны быть заперты, и внешняя защита должна быть предусмотрена для окон, особенно если они находятся на уровне земли;

г) должна быть выделена и укомплектована персоналом зона регистрации посетителей, или должны существовать другие меры для контроля физического доступа в помещения или здания; доступ в помещения и здания должен предоставляться только авторизованному персоналу;

д) где необходимо, должны быть построены физические барьеры, предотвращающие неавторизованный физический доступ и загрязнение окружающей среды;

е) все аварийные выходы на случай пожара в периметре безопасности должны быть оборудованы аварийной сигнализацией, должны подвергаться мониторингу и тестированию вместе со стенами, чтобы создать требуемый уровень устойчивости в соответствии с применимыми региональными, национальными и международными стандартами; они должны эксплуатироваться в соответствии с местной системой противопожарных правил безотказным образом;

ж) следует устанавливать необходимые системы обнаружения вторжения, соответствующие национальным, региональным или международным стандартам, и регулярно тестировать их на предмет охвата всех внешних дверей и доступных окон, свободные помещения необходимо ставить на сигнализацию; аналогично следует оборудовать и другие зоны, например серверную комнату или помещение, где расположены средства коммуникаций;

з) необходимо физически изолировать средства обработки информации, контролируемые организацией, от средств, контролируемых сторонними организациями.

Физическая защита может быть обеспечена созданием одного или нескольких физических барьеров вокруг помещений и средств обработки информации органа внутренних дел. Использование нескольких барьеров дает дополнительную защиту, и повреждение одного барьера не означает немедленного нарушения безопасности.

Зоной безопасности может быть запираемое служебное помещение или несколько помещений внутри физического барьера безопасности. Между зонами с различными требованиями безопасности, находящимися внутри периметра безопасности, могут потребоваться дополнительные барьеры и периметры для контроля физического доступа.

В отношении безопасности физического доступа особое внимание следует обращать на здания, в которых размещено несколько организаций.



6.1.2. Меры и средства контроля и управления физическим входом

Зоны безопасности необходимо защищать с помощью соответствующих мер и средств контроля и управления входа, чтобы обеспечить уверенность в том, что доступ разрешен только авторизованному персоналу.

Следует принимать во внимание следующие рекомендации:

а) дату и время входа и выхода посетителей следует регистрировать, и всех посетителей необходимо сопровождать, или они должны обладать соответствующим пропуском; доступ следует предоставлять только для выполнения определенных авторизованных задач, а также необходимо инструктировать посетителей на предмет требований безопасности, и действий в случае аварийных ситуаций;

б) доступ к зонам, где обрабатывается или хранится чувствительная информация, должен контролироваться и предоставляться только авторизованным лицам; следует использовать средства аутентификации, например контрольную карту доступа с персональным идентификационным номером (ПИН) для авторизации и проверки всех видов доступа; необходимо вести защищенные контрольные записи регистрации доступа;

в) необходимо требовать, чтобы все сотрудники, подрядчики и представители третьей стороны носили ту или иную форму видимого идентификатора и незамедлительно уведомляли сотрудников службы безопасности о замеченных несопровождаемых посетителях и лицах, не носящих видимого идентификатора;

г) доступ в зоны безопасности или к средствам обработки чувствительной информации персоналу вспомогательных служб третьей стороны следует предоставлять только при необходимости; такой доступ должен быть санкционирован и сопровождаться соответствующим контролем;

д) права доступа в зоны безопасности следует регулярно анализировать, пересматривать, и аннулировать при необходимости.

6.1.3. Безопасность зданий, служебных помещений и оборудования

Необходимо разработать и реализовать физическую защиту зданий, служебных помещений и оборудования.

В отношении защиты зданий, служебных помещений и оборудования необходимо учитывать следующие рекомендации:

а) следует принимать в расчет соответствующие правила и стандарты, касающиеся охраны здоровья и безопасности труда;

б) основное оборудование должно быть расположено в местах, где ограничен доступ посторонним лицам;

в) здания, где это применимо, должны давать минимальную информацию относительно их предназначения, не должны иметь явных признаков снаружи или внутри здания, позволяющих установить наличие деятельности по обработке информации;

г) справочники и внутренние телефонные книги, указывающие на местоположение средств обработки чувствительной информации, не должны быть легкодоступными для посторонних лиц.

6.1.4. Защита от внешних угроз и угроз со стороны окружающей среды

Необходимо разработать и реализовать физическую защиту от нанесения ущерба, который может явиться результатом пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий.

Необходимо предусмотреть любые угрозы безопасности, исходящие от соседних помещений, например пожар в соседнем здании, воду, текущую с крыши или затопившую этажи, находящиеся ниже уровня земли, или взрыв на улице.

Для предотвращения ущерба от пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий, следует учитывать следующие рекомендации:

а) обеспечить надежное хранение опасных или горючих материалов на достаточном расстоянии от охраняемой зоны; боль-

шие запасы, например бумаги для печатающих устройств, не следует хранить в пределах зоны безопасности;

б) резервное оборудование и носители данных следует размещать на безопасном расстоянии во избежание повреждения от последствия стихийного бедствия в основном здании;

в) следует обеспечить и соответствующим образом разместить необходимые средства пожаротушения.

6.1.5. Работа в зонах безопасности

Необходимо разработать и реализовать физическую защиту и рекомендации по работе в зонах безопасности.

Необходимо рассмотреть следующие рекомендации:

а) о существовании зоны безопасности и проводимых там работах персонал должен быть осведомлен по «принципу необходимого знания»;

б) из соображений безопасности и предотвращения возможности злонамеренных действий в зонах безопасности необходимо избегать выполнения работы без надлежащего контроля со стороны уполномоченного персонала;

в) пустующие зоны безопасности должны быть физически заперты и их состояние необходимо периодически проверять;

г) использование фото-, видео-, аудио- и другого записывающего оборудования, например камер, имеющих в мобильных устройствах, должно быть запрещено, если только на это не получено специальное разрешение.

Меры и средства контроля и управления, связанные с работой в зонах безопасности, включают в себя меры и средства контроля и управления, применяемые в отношении сотрудников, подрядчиков и представителей третьей стороны, работающих в зоне безопасности, а также в отношении других видов деятельности третьей стороны, выполняемых там.

6.1.6. Зоны общего доступа, приемки и отгрузки

Места доступа, например зоны приемки и отгрузки, и другие места, где неавторизованные лица могут проникнуть в помещения, должны находиться под контролем и, по возможности, должны быть изолированы от средств обработки информации, во избежание неавторизованного доступа.

Необходимо рассмотреть следующие рекомендации:

а) доступ к зоне приемки и отгрузки с внешней стороны здания должен быть разрешен только определенному и авторизованному персоналу;

б) зона приемки и отгрузки должна быть организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;

в) должна быть обеспечена безопасность внешних дверей зоны приемки и отгрузки в то время, когда внутренние двери открыты;

г) поступающие материальные ценности должны быть проверены на предмет потенциальных угроз прежде, чем они будут перемещены из зоны приемки и отгрузки к месту использования;

д) при поступлении материальные ценности должны регистрироваться в соответствии с процедурами управления активами;

е) там, где возможно, ввозимые и вывозимые грузы должны быть физически разделены.

6.2. Безопасность оборудования

Цель: Предотвращать потерю, повреждение, кражу или компрометацию активов и прерывание деятельности органа внутренних дел.

Оборудование необходимо защищать от физических угроз и воздействия окружающей среды.

Обеспечение безопасности оборудования (включая используемое вне органа внутренних дел и выносимое имущество) необходимо для уменьшения риска неавторизованного доступа к информации и защиты ее от потери или повреждения. При этом следует учесть размещение и утилизацию оборудования. Могут

потребуется специальные меры и средства контроля и управления для защиты от физических угроз, а также для защиты инфраструктуры поддерживающих услуг, например системы электропитания и кабельной разводки.

6.2.1. Размещение и защита оборудования

Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от угроз окружающей среды и возможности неавторизованного доступа.

Необходимо рассмотреть следующие рекомендации по защите оборудования:

а) оборудование следует размещать таким образом, чтобы свести к минимуму излишний доступ в рабочие зоны;

б) средства обработки информации, обрабатывающие чувствительные данные, следует размещать и ограничивать угол обзора таким образом, чтобы уменьшить риск просмотра информации неавторизованными лицами во время их использования, а средства хранения информации следует защищать от неавторизованного доступа;

в) отдельные элементы оборудования, требующие специальной защиты, следует изолировать для снижения общего уровня требуемой защиты;

г) меры и средства контроля и управления должны быть внедрены таким образом, чтобы свести к минимуму риск потенциальных физических угроз (воровство, пожар, взрывы, задымление, затопление или неисправность водоснабжения, пыль, вибрация, химическое воздействие, помехи в электроснабжении, помехи в работе линий связи, электромагнитное излучение и вандализм);

д) необходимо устанавливать правила в отношении приема пищи, питья и курения вблизи средств обработки информации;

е) следует проводить мониторинг состояния окружающей среды по выявлению условий, например температуры и влажности, которые могли бы оказать неблагоприятное влияние на функционирование средств обработки информации;

ж) на всех зданиях должна быть установлена защита от молнии, а фильтры защиты от молнии должны быть установлены на входе всех линий электропередачи и линий коммуникации;

з) оборудование, обрабатывающее чувствительную информацию, должно быть защищено, чтобы свести к минимуму риск утечки информации вследствие излучения.

6.2.2. Поддерживающие услуги

Оборудование необходимо защищать от перебоев подачи электроэнергии и других сбоев, связанных с перебоями в обеспечении поддерживающих услуг.

Все поддерживающие услуги, например электроснабжение, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха, должны быть адекватными для поддерживаемых ими систем. Объекты поддерживающих услуг необходимо регулярно проверять и тестировать для обеспечения уверенности в их должном функционировании и уменьшения любого риска, связанного с их неисправной работой или отказом. Необходимо обеспечить надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Оборудование, поддерживающее важнейшие процессы служебной деятельности, рекомендуется подключать через источники бесперебойного электропитания (далее – ИБП), чтобы обеспечить его безопасное выключение и/или непрерывное функционирование. В планах обеспечения непрерывности электроснабжения следует предусмотреть действия на случай отказа ИБП. Резервный генератор следует использовать, когда функционирование оборудования необходимо обеспечить во время длительного отказа подачи электроэнергии. Для обеспечения работы генератора в течение длительного времени необходимо обеспечить соответствующую поставку топлива. Оборудование ИБП и генераторы должны регулярно проверяться, чтобы обеспечить уверенность в наличии адекватной производительности, а также тестироваться в соответствии с рекомендациями производителя. Кроме того, следует обращать внимание на использование нескольких источников питания или, если организация большая, отдельной электроподстанции.

Аварийные выключатели электропитания необходимо расположить около запасных выходов помещений, в которых находится оборудование, чтобы ускорить отключение электропитания в критических ситуациях. Необходимо обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

Водоснабжение должно быть стабильным и адекватным для обеспечения кондиционирования воздуха, обеспечения работы устройств увлажнения и систем пожаротушения (там, где они используются). Неисправности в работе системы водоснабжения могут привести к повреждению оборудования или могут препятствовать эффективной работе системы пожаротушения. Следует оценивать необходимость установки системы сигнализации для обнаружения неправильного функционирования объектов поддерживающих услуг.

Связь телекоммуникационного оборудования с оборудованием провайдера услуг должна осуществляться, по меньшей мере, по двум различным маршрутам, чтобы предотвратить отказ в одном из соединительных маршрутов, который может сделать услугу по передаче речи невозможной. Услуги по передаче речи должны быть адекватными, чтобы удовлетворять местным законодательным требованиям в отношении аварийной связи.

Вариантом достижения непрерывности электропитания будет наличие нескольких источников питания, что позволит избежать единой точки отказа в электропитании.



6.2.3. Безопасность кабельной сети

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживающие информационные услуги, необходимо защищать от перехвата информации или разрушения.

В отношении безопасности кабельной сети следует рассмотреть следующие рекомендации:

а) силовые и телекоммуникационные линии, связанные со средством обработки информации, должны, по возможности, располагаться под землей или иметь адекватную альтернативную защиту;

б) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;

в) силовые кабели должны быть отделены от коммуникационных, чтобы предотвращать помехи;

г) следует использовать кабель и оборудование с четкой маркировкой, чтобы свести к минимуму эксплуатационные ошибки, например случайного внесения исправлений при ремонте сетевых кабелей;

д) для уменьшения вероятности ошибок следует использовать документально оформленный перечень исправлений;

е) дополнительные меры и средства контроля и управления для чувствительных или критических систем включают:

- использование армированного кабельного канала, а также закрытых помещений или шкафов в контрольных и конечных точках;

- использование дублирующих маршрутов прокладки кабеля и (или) альтернативных способов передачи, обеспечивающих соответствующую безопасность;

- использование оптико-волоконных линий связи;

- использование электромагнитного экранирования для защиты кабелей;

- проведение технических осмотров и физических проверок подключения неавторизованных устройств к кабельной сети;

- управляемый доступ к коммутационным панелям и электрощитовым.

6.2.4. Техническое обслуживание оборудования

Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности.

В отношении технического обслуживания оборудования следует рассмотреть следующие рекомендации:

а) оборудование должно обслуживаться в соответствии с рекомендуемыми поставщиком периодичностью и спецификациями;

б) техническое обслуживание и ремонт оборудования должны проводиться только авторизованным персоналом;

в) следует хранить записи обо всех предполагаемых или фактических неисправностях и всех видах профилактического обслуживания;

г) если запланировано техническое обслуживание оборудования, следует принимать соответствующие меры и средства контроля и управления, при этом необходимо учитывать, будет ли техническое обслуживание проводиться персоналом органа внутренних дел или за ее пределами; при необходимости, чувствительная информация из оборудования должна быть удалена, или специалисты по техническому обслуживанию и ремонту должны иметь соответствующий допуск.

6.2.5. Безопасность оборудования вне помещений органа внутренних дел

При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, следует учитывать различные риски, связанные с работой вне помещений органа внутренних дел.

Независимо от права собственности использование оборудования для обработки информации вне помещений органа внутренних дел должно быть санкционировано руководством.

Следующие рекомендации необходимо учитывать в отношении защиты оборудования, используемого вне помещений органа внутренних дел:

а) оборудование и носители информации, взятые из помещений органа внутренних дел, не следует оставлять без присмотра в общедоступных местах; во время поездок портативные компьютеры нужно перевозить как ручную кладь и по возможности маскировать;

б) необходимо соблюдать инструкции изготовителей по защите оборудования, например по защите от воздействия сильных электромагнитных полей;

в) для работы на дому следует определить соответствующие меры и средства контроля и управления, исходя из оценки рисков, например использование запираемых шкафов для хранения доку-

ментов, соблюдение политики «чистого стола», управление доступом к компьютерам и связь с органом внутренних дел по защищенным сетям (см. также ГОСТ Р ИСО/МЭК 27033-1-2011 [11]).

Риски безопасности, например связанные с повреждением, воровством и подслушиванием, могут значительно отличаться для различных объектов и должны учитываться при определении наиболее подходящих мер и средств контроля и управления.

Под оборудованием, используемым для обработки и хранения информации, понимаются все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, смарт-карт, а также бумага или другие виды носителей информации, которые применяются для работы на дому или транспортируются за пределы обычных служебных помещений.

6.2.6. Безопасная утилизация или повторное использование оборудования

Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые чувствительные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

Носители данных, содержащие чувствительную информацию, необходимо физически уничтожать, или информацию необходимо разрушить, удалить или перезаписать способами, делающими исходную информации невозстановимой, а не использовать стандартные функции удаления и форматирования.

Поврежденные устройства, содержащие чувствительные данные, могут потребовать проведения оценки рисков с целью определения элементов, которые должны быть физически разрушены, направлены на ремонт или игнорированы.

Информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования.

6.2.7. Перемещение имущества

Оборудование, информацию или программное обеспечение можно использовать вне помещений органа внутренних дел только при наличии соответствующего разрешения.

Необходимо учитывать следующие рекомендации:

а) оборудование, информацию или программное обеспечение можно использовать вне помещений органа внутренних дел только при наличии соответствующего разрешения;

б) сотрудники, подрядчики и представители третьей стороны, имеющие право разрешать перемещение активов за пределы места эксплуатации, должны быть четко определены;

в) сроки перемещения оборудования должны быть установлены и проверены на соответствие при возврате;

г) там, где необходимо и уместно, оборудование следует регистрировать при перемещении из помещений органа внутренних дел и при возврате.

Выборочные проверки, проводимые для обнаружения неавторизованного перемещения имущества, также могут проводиться для обнаружения неавторизованных устройств регистрации и т. д., и предотвращения их вноса в помещения органа внутренних дел. Такие выборочные проверки необходимо выполнять согласно соответствующим законам и инструкциям. Сотрудники должны быть осведомлены о проведении выборочных проверок, а проверки должны проводиться только с разрешения, соответствующего правовым и нормативным требованиям.



7. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ КОММУНИКАЦИИ

7.1. Эксплуатационные процедуры и обязанности

Цель: Обеспечить уверенность в надлежащем и безопасном функционировании средств обработки информации.

Должны быть установлены обязанности и процедуры в отношении управления и эксплуатации всех средств обработки информации, включая также разработку соответствующих эксплуатационных процедур.

С целью сведения к минимуму риска неправильного использования систем вследствие небрежности или злого умысла, следует, по возможности, реализовать принцип разграничения обязанностей.

7.1.1. Документальное оформление эксплуатационных процедур

Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.

Документально оформленные процедуры должны быть подготовлены для действий системы, связанных со средствами обработки информации и связи, таких как процедуры запуска и завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обращения с носителями информации, управление работой в машинном зале и работы с почтой, а также процедуры обеспечения безопасности.

Данные процедуры должны содержать детальные инструкции по выполнению каждой работы, включая:

- а) обработку и управление информацией;
- б) резервирование;
- в) требования в отношении графика работ, включая взаимозависимости между системами, время начала самой ранней работы и время завершения самой последней работы;

г) инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит;

д) необходимые контакты на случай неожиданных эксплуатационных или технических проблем;

е) специальные инструкции по управлению выводом данных и обращению с носителями информации, например использование специальной бумаги для печатающих устройств или управление выводом конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе;

ж) перезапуск системы и соответствующие процедуры восстановления на случай системных сбоев;

з) управление информацией, содержащейся в контрольных записях и системных журналах.

Эксплуатационные процедуры и документально оформленные процедуры действий системы должны рассматриваться как официальные документы, а изменения в них должны санкционироваться руководством. Если технически возможно, управление информационных систем необходимо осуществлять единообразно, используя одни и те же процедуры, инструментальные средства и утилиты.

7.1.2. Управление изменениями

Изменения в конфигурации средств обработки информации и системах должны контролироваться.

Эксплуатируемые системы и прикладное программное обеспечение должны быть предметом строгого контроля управления изменениями.

В частности, необходимо рассмотреть следующие аспекты:

- а) определение и регистрацию существенных изменений;
- б) планирование и тестирование изменений;
- в) оценку возможных последствий, включая последствия для безопасности, таких изменений;
- г) формализованную процедуру утверждения предполагаемых изменений;

д) подробное информирование об изменениях всех заинтересованных лиц;

е) процедуры возврата в исходный режим, включая процедуры и обязанности в отношении отмены и последующего восстановления в случае неудачных изменений и непредвиденных обстоятельств.

С целью обеспечения уверенности в надлежащем контроле всех изменений в оборудовании, программном обеспечении или процедурах, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в контрольном журнале.

Неадекватный контроль изменений средств и систем обработки информации - распространенная причина системных сбоев и инцидентов безопасности. Изменения эксплуатационной среды, особенно при переходе от стадии разработки к стадии эксплуатации, могут оказывать влияние на надежность прикладных программ.

Изменения эксплуатируемых систем следует осуществлять только в том случае, если на это имеется обоснованная причина, затрагивающая бизнес, например возрастание риска в отношении системы. Обновление систем новейшими версиями эксплуатируемой системы или прикладных программ не всегда отвечает интересам служебной деятельности, поскольку оно может привести к большему числу уязвимостей и большую нестабильность, чем действующая версия.

Могут также потребоваться дополнительное обучение, расходы на лицензирование, поддержка, сопровождение и административный надзор, а также аппаратные средства, особенно в течение периода миграции.

7.1.3. Разделение обязанностей

Обязанности и области ответственности должны быть разделены для уменьшения возможностей неавторизованной или непреднамеренной модификации активов организации или их нецелевого использования.

Разделение обязанностей – это способ сведения к минимуму риска нецелевого использования систем вследствие ошибочных или злонамеренных действий пользователей. Необходимо предпринять определенные меры предосторожности, чтобы ни один сотрудник не мог осуществлять доступ, модифицировать или использовать активы, не имея авторизации или не будучи обнаруженным. Инициирование события должно быть отделено от его авторизации. При разработке мер и средств контроля и управления следует учитывать опасность сговора.

Небольшие органы внутренних дел могут признавать разделение обязанностей труднодостижимым, однако, данный принцип должен быть применен насколько это возможно. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование альтернативных мер и средств контроля и управления, таких как мониторинг деятельности, использование контрольных записей, а также надзор со стороны руководства. В то же время важно, чтобы аудит безопасности оставался независимым.

7.1.4. Разделение средств разработки, тестирования и эксплуатации

Чтобы снизить риски неавторизованного доступа или изменений эксплуатируемой системы, следует обеспечивать разделение средств разработки, тестирования и эксплуатации.

Уровень разделения между средами эксплуатации, тестирования и разработки, необходимый для предотвращения проблем эксплуатации, должен быть определен и при этом должны быть реализованы соответствующие меры и средства контроля и управления.

Необходимо рассмотреть следующие вопросы:

а) правила перевода программного обеспечения из статуса, разрабатываемого в статус принятого к эксплуатации, должны быть определены и документально оформлены;

б) разработка и эксплуатация программного обеспечения должна осуществляться на различных системах или компьютерах в различных доменах или директориях;

в) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должны быть доступны в среде эксплуатации без крайней необходимости;

г) среда системы тестирования должна эмулировать среду эксплуатации настолько точно, насколько это возможно;

д) чтобы уменьшить риск ошибок, пользователи должны применять различные параметры пользователя для эксплуатируемых и тестовых систем, а в экранном меню должны показываться соответствующие идентификационные сообщения;

е) чувствительные данные не должны копироваться в среду системы тестирования.

Деятельность, связанная с разработкой и тестированием, может быть причиной серьезных проблем, например нежелательных изменений файлов или системной среды, а также системных сбоев. В этом случае необходимо поддерживать известную и стабильную среду для выполнения комплексного тестирования и предотвращать несанкционированный доступ разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к действующей системе и ее данным, они могут установить неавторизованную и протестированную программу или изменить рабочие данные. Применительно к ряду систем такая возможность могла бы быть использована для мошенничества или установки протестированной или вредоносной программы, что может являться причиной серьезных проблем, связанных с эксплуатацией.

Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз конфиденциальности эксплуатационной информации. Кроме того, если разработка и тестирование производятся в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения или информации. Следовательно, разделение средств разработки, тестирования и эксплуатации целесообразно для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и данным служебной деятельности среды эксплуатации.

7.2. Управление оказанием услуг третьей стороной

Цель: Реализовывать и поддерживать соответствующий уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг третьей стороной.

Орган внутренних дел должен проводить проверку реализации договоров, осуществлять мониторинг соответствия условиям договоров и управление изменениями для обеспечения уверенности в том, что оказанные услуги удовлетворяют всем требованиям, согласованным с третьей стороной.

7.2.1. Предоставление услуг

Необходимо обеспечивать уверенность в том, что меры и средства контроля и управления безопасности, определение услуг и уровни предоставления услуг, включенные в договор о предоставлении услуг третьей стороной, реализуются, функционируют и поддерживаются третьей стороной.

Предоставление услуг третьей стороной должно включать согласованные меры по обеспечению безопасности, определению услуг и аспекты управления услугами. Что касается договоров аутсорсинга, орган внутренних дел должен планировать необходимые перемещения (информации, средств обработки информации и др., что должно быть перемещено) и обеспечивать уверенность в том, что безопасность поддерживается на протяжении всего периода перемещения.

Орган внутренних дел должен обеспечивать уверенность в том, что третья сторона поддерживает достаточный объем услуг наряду с реализуемыми планами по обеспечению согласованного уровня непрерывности обслуживания, сохраняемого в случае серьезных отказов обслуживания или бедствия.

7.2.2. Мониторинг и анализ услуг третьей стороны

Необходимо регулярно проводить мониторинг и анализ услуг, отчетов и записей, обеспечиваемых третьей стороной, и регулярно проводить аудиты.

Мониторинг и анализ услуг, обеспечиваемых третьей стороной, должны обеспечивать уверенность в том, что условия, касающиеся информационной безопасности, и условия договоров соблюдаются, и что управление инцидентов и проблем информационной безопасности осуществляется должным образом. Между органом внутренних дел и третьей стороной должна существовать связь для того, чтобы:

а) осуществлять мониторинг уровней предоставления услуг с целью проверки соблюдения условий договоров;

б) анализировать отчеты о предоставлении услуг, подготовленные третьей стороной, и проводить регулярные рабочие встречи в соответствии с договорами;

в) обеспечивать информацию об инцидентах информационной безопасности и анализ данной информации третьей стороной и органом внутренних дел в соответствии с условиями договоров и любыми поддерживающими руководствами и процедурами;

г) анализировать контрольные записи третьей стороны и записи событий, связанных с безопасностью, эксплуатационных проблем, отказов, прослеживания недостатков и разрушений, относящихся к предоставляемым услугам;

д) решать все выявленные проблемы и осуществлять их управление.

Ответственность за управление отношениями с третьей стороной следует возлагать на специально назначенного сотрудника или на группу управления услугами. Кроме того, орган внутренних дел должен обеспечивать уверенность в том, что третья сторона берет на себя ответственность за проверку соответствия и исполнения требований договоров. Для мониторинга выполнения требований договора, в частности, требований информационной безопасности, необходимы достаточный технический опыт и ресурсы. Когда в оказании услуг замечены недостатки, следует принимать соответствующие меры.

Орган внутренних дел должен поддерживать достаточный общий контроль и прослеживаемость всех аспектов безопасности чувствительной или критической информации, или средств обработки информации, которые доступны, обрабатываются или управляются третьей стороной. Орган внутренних дел должен обеспечивать уверенность в том, что он поддерживает прослежи-

ваемость деятельности, связанной с безопасностью, например управление изменениями, выявление уязвимостей и сообщение/реагирование на инциденты информационной безопасности с помощью четко определенного процесса, формата и структуры отчетности.

Орган внутренних дел должен быть осведомлен о том, что основная ответственность за информацию, обрабатываемую третьей стороной в рамках договоров аутсорсинга, остается за органом внутренних дел.



7.2.3. Управление изменениями услуг третьей стороны

Изменения в предоставлении услуг, включая поддержку и улучшение существующих политик, процедур, мер и средств контроля и управления информационной безопасности, должны осуществляться с учетом критичности затрагиваемых систем и процессов служебной деятельности, а также переоценки рисков.

Процесс управления изменениями услуг третьей стороны должен учитывать:

а) изменения, проводимые органом внутренних дел, для реализации:

- повышения эффективности служебной деятельности;
- разработки каких-либо новых прикладных программ и систем;
- модификаций или обновлений политик и процедур орган внутренних дел;
- новых мер и средств контроля и управления для устранения инцидентов информационной безопасности и повышения безопасности;

б) изменения в услугах третьей стороны, для реализации:

- изменений и улучшений в отношении сетей;
- использования новых технологий;
- использования новых продуктов или новейших версий/выпусков;
- новых инструментальных средств и сред разработки;
- изменений физического расположения средств обслуживания;
- смены поставщиков.

7.3. Планирование и приемка систем

Цель: Свести к минимуму риск сбоев в работе систем.

Предварительное планирование и подготовка необходимы для обеспечения адекватной производительности и ресурсов, чтобы получить требуемые эксплуатационные данные системы.

Необходимо составить прогноз в отношении требований и перспективной производительности систем с целью снижения риска их перегрузки.

Эксплуатационные требования для новых систем должны быть определены, документально оформлены и протестированы перед их приемкой и использованием.

7.3.1. Управление производительностью

Использование ресурсов необходимо прогнозировать, исходя из будущих требований к производительности, настраивать и контролировать, чтобы обеспечить уверенность в достижении требуемых эксплуатационных данных системы.

Для каждой новой и продолжающейся деятельности необходимо определять требования к производительности. Следует проводить настройку и контроль систем для обеспечения, где необходимо, уверенности в повышении доступности и эффективности систем. Необходимо применять выявляющие меры и средства контроля и управления, своевременно указывающие на проблемы. Прогнозирование требований к производительности должно учитывать новые требования служебной деятельности и новые системные требования, а также текущие и прогнозируемые тенденции в отношении возможностей обработки информации органа внутренних дел.

Особое внимание необходимо уделять любым ресурсам, требующим длительного времени на закупку или больших расходов, поэтому руководителям следует осуществлять контроль использования ключевых системных ресурсов. Они должны определять тенденции в использовании, в частности, касающиеся прикладных программ для служебной деятельности или инструментальных средств информационных систем управления.

Руководителям следует использовать эту информацию с целью выявления потенциально узких мест и зависимости от ключевого персонала, который мог бы представлять угрозу безопасности систем или сервисов, и планирования соответствующего действия.

7.3.2. Приемка систем

Должны быть определены критерии приемки для новых информационных систем, обновлений и новых версий, кроме того, необходимо тестировать системы в течение их разработки и перед их приемкой.

Руководители должны обеспечить уверенность в том, что требования и критерии для принятия новых систем четко определены, согласованы, документально оформлены и протестированы. Новые информационные системы, обновления и новые версии должны вводиться в эксплуатацию только после прохождения официальной приемки. До официальной приемки необходимо рассмотреть следующие аспекты:

- а) требования к мощности и производительности компьютера;
- б) процедуры восстановления после сбоев и перезапуска, и планы действий в чрезвычайных ситуациях;
- в) подготовка и тестирование типовых операционных процедур на соответствие установленным стандартам;
- г) наличие согласованного набора меры и средства контроля и управления безопасности;
- д) эффективные ручные процедуры;
- е) мероприятия по обеспечению непрерывности служебной деятельности;
- ж) документальное подтверждение того, что внедрение новой системы не будет неблагоприятно влиять на существующие системы, особенно, во время максимальных нагрузок, например в конце месяца;
- з) документальное подтверждение того, что было учтено влияние, оказываемое новой системой, на общую безопасность орган внутренних дел;
- и) тренинг в отношении эксплуатации и использования новых систем;

к) простота использования, поскольку это влияет на производительность работы пользователя и позволяет избегать ошибок оператора.

В отношении новых крупных разработок, службы поддержки и пользователи должны привлекаться для консультации на всех стадиях процесса разработки с целью эффективного проектирования системы. Соответствующие тесты должны проводиться для подтверждения того, что все критерии приемки удовлетворены полностью.

Приемка может включать формальный процесс сертификации и аккредитации для подтверждения того, что требования к безопасности были учтены должным образом.



7.4. Защита от вредоносных и мобильных программ

Цель: Защита целостности программного обеспечения и информации.

Необходимо принимать меры предосторожности для предотвращения и обнаружения вредоносной программы и неавторизованной мобильной программы.

Программное обеспечение и средства обработки информации уязвимы по отношению к внедрению вредоносной программы, такой как компьютерные вирусы, сетевые «черви», «тройные кони» и логические бомбы. Пользователи должны быть осведомлены об опасности, связанной с вредоносной программой. Руководители должны, при необходимости, обеспечить внедрение мер и средств контроля и управления с целью предотвращения, обнаружения и удаления вредоносной программы и контролирования мобильной программы.

7.4.1. Меры и средства контроля и управления против вредоносной программы

Необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей.

Защита от вредоносной программы должна основываться: на обнаружении вредоносной программы и восстановлении программного обеспечения; на понимании требований безопасности; на мерах и средствах контроля и управления соответствующего доступа к системе и управления изменениями. Необходимо рассмотреть следующие рекомендации:

а) создать официальную политику, устанавливающую запрет на использование неавторизованного программного обеспечения;

б) создать официальную политику защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через другие передающие среды, показывающую, какие защитные меры следует принять;

в) проводить регулярный анализ программного обеспечения и содержания данных систем, поддерживающих критические процессы служебной деятельности; необходима формальная процедура расследования причин наличия любых неавторизованных или измененных файлов;

г) осуществлять в качестве превентивной меры или обычным порядком установку и регулярное обновление программного обеспечения по обнаружению вредоносной программы и восстановлению для сканирования компьютеров и носителей информации; проводимые проверки должны включать:

- проверку на наличие вредоносной программы любых файлов на электронных или оптических носителях и файлов, полученных из сетей перед их использованием;

- проверку любых вложений электронной почты и скачиваемой информации до их использования на наличие вредоносной программы; эта проверка должна выполняться в разных точках, например на серверах электронной почты, настольных компьютерах или при входе в сеть органа внутренних дел;

- проверку web-страниц на наличие вредоносной программы;

д) определять управленческие процедуры и обязанности, связанные с защитой от вредоносной программы в системах, тренинг их использования, оповещение и восстановление после атак вредоносной программы;

е) подготовить соответствующие планы по обеспечению непрерывности служебной деятельности в части восстановления после атак вредоносной программы, включая все необходимые

мероприятия по резервированию и восстановлению данных и программного обеспечения;

ж) реализовать процедуры регулярного сбора информации, например подписываясь на список почтовой рассылки и (или) проверяя web-сайты, дающие информацию о новой вредоносной программе;

з) реализовать процедуры проверки информации, касающейся вредоносной программы, и обеспечить точность и информативность предупредительных сообщений; соответствующие руководители должны обеспечить уверенность в том, что компетентные источники, например информация из известных журналов, заслуживающих доверия Интернет-сайтов или от поставщиков антивирусного программного обеспечения используется для определения различий между ложной и реальной вредоносной программой; все пользователи должны быть осведомлены о проблеме ложных вирусов и действиях при их получении.

Использование двух или более программных продуктов, обеспечивающих защиту от вредоносной программы в среде обработки информации, от разных поставщиков может повысить эффективность данной защиты.

Для защиты от вредоносной программы может устанавливаться программное обеспечение, позволяющее проводить автоматические обновления определенных файлов и сканирование машин для подтверждения актуальности защиты. Кроме того, такое программное обеспечение может быть установлено на каждом рабочем столе для выполнения автоматических проверок.

Следует заботиться о защите от внедрения вредоносной программы во время процедур по техническому обслуживанию и процедур, связанных с критическими ситуациями, когда можно обойти обычные меры и средства контроля и управления, применяемые для защиты от вредоносной программы.



7.4.2. Меры и средства контроля и управления при использовании мобильной программы

Там, где разрешено использование мобильной программы, конфигурация должна обеспечивать уверенность в том, что разрешенная мобильная программа функционирует в соответствии с ясно сформулированной политикой безопасности, а исполнение неразрешенной мобильной программы будет запрещено.

Для предотвращения выполнения мобильной программой неразрешенных действий необходимо принимать следующие меры:

- а) обеспечивать выполнение мобильной программы в логически изолированной среде;
- б) блокировать любое несанкционированное использование мобильной программы;
- в) блокировать прием мобильной программы;
- г) активизировать технические меры, доступные в отношении определенной системы, чтобы обеспечить уверенность в управляемости мобильной программы;
- д) контролировать ресурсы, доступные мобильной программе;
- е) применять криптографические меры и средства контроля и управления для однозначной аутентификации мобильной программы.

Мобильная программа представляет собой программный код, который переходит с одного компьютера на другой, а затем исполняется автоматически, и выполняет определенную функцию без какого-либо взаимодействия с пользователем или при минимальном взаимодействии с ним. Мобильная программа связана с рядом услуг вспомогательного программного обеспечения.

В дополнение к обеспечению уверенности в том, что мобильная программа не содержит вредоносного кода, важно контролировать мобильную программу с целью предотвращения неавторизованного использования или разрушения системных, сетевых или прикладных ресурсов и других нарушений информационной безопасности.



7.5. Резервирование

Цель: Поддерживать целостность и доступность информации и средств обработки информации.

Должны быть созданы типовые процедуры по реализации установленной политики и стратегии резервирования в отношении снятия резервных копий данных и обеспечения их своевременного восстановления.

Резервное копирование информации и программного обеспечения должно выполняться и тестироваться на регулярной основе в соответствии с установленной политикой резервирования.

Следует обеспечить адекватные средства резервирования для обеспечения уверенности в том, что вся важная информация и программное обеспечение могут быть восстановлены после бедствия или сбоя оборудования.

В отношении резервирования информации необходимо рассматривать следующие вопросы:

а) необходимо определить надлежащий уровень резервной информации;

б) необходимо обеспечивать точные и полные записи резервных копий и документально оформленные процедуры восстановления;

в) объем (т. е. полное или выборочное резервирование) и частота резервирования должны отражать требования служебной деятельности орган внутренних дел, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы органа внутренних дел;

г) резервные копии должны храниться в удаленном месте, на надежном расстоянии, достаточном, чтобы избежать любого повреждения вследствие аварийной ситуации в основном здании;

д) в отношении резервной информации должен быть обеспечен соответствующий уровень физической защиты и защиты от воздействий окружающей среды, в соответствии со стандартами, применяемыми в основном здании; меры и средства контроля и управления, применяемые к носителям информации в основном здании, должны также применяться и на резервной площадке;

е) носители резервной информации должны регулярно тестироваться для обеспечения уверенности в том, что в случае чрезвычайных ситуаций они могут быть использованы;

ж) процедуры восстановления следует регулярно проверять и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем это определено;

з) в ситуациях, когда конфиденциальность играет важную роль, резервные копии необходимо защищать посредством шифрования.

Мероприятия по резервированию, применяемые в отношении отдельных систем, должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям, содержащимся в планах непрерывности служебной деятельности. Применительно к критическим системам, мероприятия по резервированию должны охватывать информацию, прикладные программы и данные всех систем, необходимые для восстановления целой системы в случае бедствия.

Следует определить сроки хранения важной информации служебной деятельности, а также любое требование к архивным копиям, подлежащим длительному хранению.

Для упрощения процесса резервирования и восстановления мероприятия по резервированию могут быть автоматизированы. Такие решения по автоматизации должны в достаточной мере и регулярно тестироваться, прежде чем они будут реализованы.



7.6. Управление безопасностью сети

Цель: Обеспечить уверенность в защите информации в сетях и защите поддерживающей инфраструктуры.

Управление безопасности сетей, которые могут проходить за пределами органа внутренних дел, требует пристального внимания к потокам данных, правовым последствиям, мониторингу и защите.

Дополнительные меры и средства контроля и управления могут также потребоваться для защиты чувствительной информации, передаваемой по общедоступным сетям.

7.6.1. Меры и средства контроля и управления сетями

Сети должны адекватно управляться и контролироваться, чтобы быть защищенными от угроз и обеспечить безопасность систем и прикладных программ, использующих сеть, включая информацию во время ее передачи.

Руководители, отвечающие за поддержку сетевых ресурсов, должны внедрять меры и средства контроля и управления для обеспечения уверенности в безопасности информации в сетях и защиты подключенных сервисов от неавторизованного доступа. В частности, необходимо рассмотреть следующие вопросы:

а) следует разделить, где это необходимо, ответственность за поддержку сетевых ресурсов и за поддержку компьютерных операций;

б) следует определить обязанности и процедуры для управления удаленным оборудованием, включая оборудование, установленное у конечных пользователей;

в) специальные меры и средства контроля и управления следует внедрить для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, или по беспроводным сетям, а также для защиты подключенных систем и прикладных программ; специальные меры и средства контроля и управления могут потребоваться для поддержки доступности сетевых сервисов и рабочих станций;

г) соответствующая регистрация и мониторинг должны применяться с целью обеспечения возможности регистрации действий, имеющих значение для безопасности;

д) действия руководства должны быть тщательно согласованы как для оптимизации получаемых органом внутренних дел услуг, так и для обеспечения уверенности в том, что меры и средства контроля и управления единообразно применимы ко всей инфраструктуре обработки информации.

Дополнительную информацию о сетевой безопасности можно найти в ГОСТ Р ИСО/МЭК 27033 [11-13].

!

7.6.2. Безопасность сетевых услуг

Средства обеспечения безопасности, уровни услуг и требования в отношении управления всех сетевых услуг должны быть определены и включены в любой договор по сетевым услугам, вне зависимости от того, будут ли они обеспечиваться силами органа внутренних дел или в рамках договоров аутсорсинга.

Способность провайдера сетевых услуг безопасно осуществлять управление установленных услуг следует определять и подвергать регулярному мониторингу, а право проведения аудита должно быть согласовано.

Должны быть определены меры безопасности, необходимые для конкретных услуг, например средства обеспечения безопасности, уровни услуг и требования в отношении управления. Орган внутренних дел должен обеспечивать уверенность в том, что провайдеры сетевых услуг реализуют эти меры.

Сетевые услуги включают в себя обеспечение соединений, услуг локальных сетей и сетей с дополнительными функциями, а также решений, касающихся управления безопасностью сети, например межсетевые экраны и системы обнаружения вторжения. Такие услуги могут варьироваться от простых решений, касающихся неуправляемой пропускной способности, до сложных решений с обеспечением дополнительных услуг.

Средствами обеспечения безопасности сетевых услуг могут быть:

а) средства, применяемые для обеспечения безопасности сетевых услуг, например аутентификация, шифрование, и меры и средства контроля и управления сетевыми соединениями;

б) соблюдение технических параметров, требуемых для безопасного подключения сетевых услуг в соответствии с правилами безопасности сетевых соединений;

в) процедуры использования сетевой услуги, применяемые для ограничения доступа к сетевым услугам или прикладным программам, где это необходимо.

7.7. Обращение с носителями информации

Цель: Предотвратить неавторизованное раскрытие, модификацию, выбытие или уничтожение активов и прерывание служебной деятельности.

Использование носителей информации должно контролироваться, а также необходимо обеспечение их физической безопасности.

Должны быть определены соответствующие процедуры в отношении защиты документов, компьютерных носителей информации (например, дисков), данных ввода/вывода и системной документации от неавторизованного раскрытия, модификации, выноса и уничтожения.

7.7.1. Управление сменными носителями информации

Должны существовать процедуры в отношении управления сменными носителями информации.

Необходимо рассмотреть следующие рекомендации в отношении управления сменными носителями информации:

а) если не предполагается повторно использовать содержание носителей информации, которые должны быть перемещены за пределы органа внутренних дел, то информацию необходимо сделать неизвлекаемой;

б) где необходимо и практично, должно требоваться разрешение на вынос носителей информации из органа внутренних дел и запись о таком перемещении следует хранить как контрольную запись для аудита;

в) все носители информации должны храниться в надежной, безопасной среде, в соответствии со спецификациями изготовителей;

г) информацию, хранимую на носителях, востребованную дольше, чем жизненный цикл носителя (в соответствии со спецификациями изготовителей), следует хранить также и в другом месте, во избежание потери информации вследствие износа носителей;

д) для уменьшения возможности потери данных должна быть предусмотрена регистрация сменных носителей информации;

е) сменные дисковые накопители разрешается использовать только в случае, обусловленном потребностями служебной деятельности.

Все процедуры и уровни авторизации должны быть четко зафиксированы документально.

К сменным носителям информации относятся ленты, диски, диски флэш-памяти, сменные жесткие диски, CD, DVD и печатные носители информации.



7.7.2. Утилизация носителей информации

Носители информации, когда в них больше нет необходимости, следует надежно и безопасно утилизировать, используя формальные процедуры.

Формальные процедуры для безопасной утилизации носителей информации должны снижать риск утечки чувствительной информации неавторизованным лицам. Процедуры для безопасной утилизации носителей, содержащих чувствительную информацию, должны соответствовать чувствительности той информации. Необходимо рассмотреть следующие вопросы:

а) носители, содержащие чувствительную информацию, должны храниться и утилизироваться надежно и безопасно, например посредством сжигания или измельчения; если носители планируется использовать в пределах органа внутренних дел для других прикладных программ, информация на них должна быть уничтожена;

б) должны существовать процедуры по выявлению носителей информации, для которых может потребоваться безопасная утилизация;

в) может оказаться проще принимать меры по сбору и безопасной утилизации в отношении всех носителей информации, чем пытаться выделить носители с чувствительной информацией;

г) многие организации предлагают услуги по сбору и утилизации бумаги, оборудования и носителей информации; следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и применяемых мер и средств контроля и управления;

д) где возможно, утилизацию носителей, содержащих чувствительную информацию, следует фиксировать как контрольную запись для аудита.

При накоплении носителей информации, подлежащих утилизации, следует принимать во внимание «эффект накопления», т. е. большое количество нечувствительной информации делает ее чувствительной.

Чувствительная информация может быть раскрыта при небрежной утилизации носителей. **!**

7.7.3. Процедуры обработки информации

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации.

Должны быть разработаны процедуры по ручной обработке информации, обработке информации с использованием компьютеров, хранению и передаче информации в соответствии с ее классификацией. Необходимо рассмотреть следующие вопросы:

а) обработку и маркировку всех носителей информации в соответствии с ее указанным уровнем классификации;

б) ограничение доступа с целью предотвращения доступа неавторизованного персонала;

в) обеспечение формальной регистрации авторизованных получателей данных;

г) обеспечение уверенности в том, что процесс ввода данных и обработки завершаются должным образом и что выполняется проверка выходных данных;

д) защиту информации, находящейся в буфере данных и ожидающей вывода, соответствующую степени чувствительности этой информации;

е) хранение носителей информации в соответствии со спецификациями изготовителей;

ж) сведение распространения данных к минимуму;

з) четкая маркировка всех копий данных, предназначенных вниманию авторизованного получателя;

и) пересмотр списков рассылки и списков авторизованных получателей через регулярные интервалы времени.

Эти процедуры применяются к информации в документах, вычислительным системам, сетям, переносным компьютерам, мобильным средствам связи, почте, речевой почте, речевой связи вообще, мультимедийным устройствам, почтовым услугам/устройствам, к использованию факсов и любых других чувствительных объектов, например бланков чеков и счетов.



7.7.4. Безопасность системной документации

Системная документация должна быть защищена от неавторизованного доступа.

Для защиты системной документации необходимо учитывать следующие вопросы:

а) системную документацию надлежит хранить безопасным образом;

б) список лиц, имеющих доступ к системной документации, необходимо свести к минимуму; доступ должен быть авторизован владельцем прикладной программы;

в) системную документацию, полученную или поддерживаемую через общедоступную сеть, следует защищать надлежащим образом.

Системная документация может содержать разнообразную чувствительную информацию, например описание процессов работы прикладных программ, процедур, структур данных, процессов авторизации.



7.8. Обмен информацией

Цель: Поддерживать безопасность информации и программного обеспечения, обмениваемых в пределах органа внутренних дел и с любым внешним объектом.

Обмен информацией и программным обеспечением между органами внутренних дел должен основываться на формальной политике обмена, осуществляться в соответствии с соглашениями по обмену и соответствовать действующему законодательству.

Необходимо определить процедуры и стандарты по защите информации и ее физических носителей при передаче.

7.8.1. Политики и процедуры обмена информацией

Должны существовать формальные политики, процедуры и меры и средства контроля и управления в отношении обмена информацией с целью защиты такого обмена, когда используются все типы средств связи.

Процедуры, меры и средства контроля и управления, которые необходимо соблюдать при использовании электронных средств связи для обмена информацией, должны учитывать следующее:

а) процедуры, предназначенные для защиты обмениваемой информации от перехвата, копирования, модификации, ложной маршрутизации и разрушения;

б) процедуры обнаружения вредоносной программы, которая может передаваться при использовании электронных средств связи, и процедуры защиты от нее;

в) процедуры защиты передаваемой чувствительной электронной информации, имеющей форму приложения;

г) политику или рекомендации, определяющие приемлемое использование электронных средств связи;

д) процедуры использования беспроводной связи, учитывая сопряженные с ней определенные риски;

е) обязательство сотрудника, подрядчика и любого другого представителя не компрометировать орган внутренних дел, например посредством клеветы, антисоциальных действий, выдачи себя за другое лицо, распространения «писем счастья», использования «тайных рычагов» и т. д.;

ж) использование криптографических методов, например для защиты конфиденциальности, целостности и аутентичности информации;

з) рекомендации по сохранению и утилизации всей служебной корреспонденции, включая сообщения, в соответствии с действующими национальными и местными законодательными и нормативными актами;

и) напоминание сотрудникам о том, что нельзя оставлять чувствительную или критическую информацию на печатающих устройствах, например копировальных устройствах, принтерах и

факсах, поскольку неавторизованный персонал может осуществлять к ним доступ;

к) меры и средства контроля и управления и ограничения, связанные с пересылкой средств связи, например автоматическая пересылка электронной почты на внешние почтовые адреса;

л) напоминание сотрудникам о необходимости соблюдения мер предосторожности, например не следует разглашать чувствительную информацию во избежание ее подслушивания или перехвата при телефонных звонках:

- лицами, находящимися в непосредственной близости, особенно при использовании мобильных телефонов;

- при прослушивании телефонных переговоров и других формах подслушивания путем физического доступа к трубке или телефонной линии, или при использовании сканирующих приемников;

- посторонними лицами на стороне адресата;

м) напоминание сотрудникам о том, что нельзя оставлять сообщения, содержащие чувствительную информацию, на автоответчиках, поскольку они могут быть прослушаны неавторизованными лицами, храниться в общественных системах или неверно помещены на хранение вследствие ошибки соединения;

н) напоминание сотрудникам о проблемах, связанных с использованием факсов, а именно:

- неавторизованный доступ к встроенной памяти для поиска сообщений;

- преднамеренное или случайное перепрограммирование аппаратов с целью передачи сообщений по определенным номерам;

- отсылка документов и сообщений по неправильному номеру вследствие ошибки в наборе, либо из-за использования неправильно сохраненного номера;

о) напоминание сотрудникам о том, что не следует регистрировать демографические данные, например адрес электронной почты или другую личную информацию, в каком-либо программном обеспечении, во избежание ее сбора для неавторизованного использования;

п) напоминание сотрудникам о том, что современные факсимильные и фотокопирующие устройства оснащены страничной кэш-памятью, и «запоминают» страницы в случае проблем с бу-

магой или передачей, которые будут напечатаны после устранения неисправности.

Кроме того, необходимо напоминать сотрудникам о том, что не следует вести конфиденциальные беседы в общественных местах или открытых офисах, а также в переговорных комнатах, стены которых не защищены звукоизоляцией.

Средства обмена информацией должны соответствовать любым действующим законодательным требованиям.

Обмен информацией может осуществляться при использовании различных типов коммуникационных средств, включая электронную почту, факсимильные, аудио- и видеосредства.

Обмен программным обеспечением может осуществляться при использовании различных типов носителей информации, включая «скачивание» из Интернета и приобретение у поставщиков, продающих готовые продукты.

Следует учитывать подразумеваемые положения служебной деятельности, законодательства и безопасности, связанные с электронным обменом данными, электронной торговлей и электронными коммуникациями, а также и с требованиями к мерам и средствам контроля и управления.

Информация может быть скомпрометирована из-за недостатка осведомленности сотрудников в отношении политики или процедур по использованию средств обмена информацией, например вследствие подслушивания при переговорах по мобильному телефону в общественном месте, отправления сообщения электронной почты по неправильному адресу, прослушивания автоответчиков, неавторизованного доступа к системам голосовой почты или случайной отсылки факсимильных сообщений неправильному адресату.

Операции служебной деятельности могут быть прерваны и информация может быть скомпрометирована в случае отказа, перегрузки или прерывания в работе средств связи. Информация может быть скомпрометирована вследствие доступа неавторизованных пользователей.

7.8.2. Соглашения по обмену информацией

Необходимо заключать соглашения по обмену информацией и программным обеспечением между органом внутренних дел и сторонними организациями.

В соглашениях по обмену следует учитывать следующие условия безопасности:

- а) обязанности руководства в отношении контроля и уведомления о передаче, отправке и получении;
- б) процедуры уведомления отправителя, а также процедуры передачи, отправки и получения;
- в) процедуры обеспечения прослеживаемости и неотказуемости;
- г) минимальные требования технических стандартов по формированию и передаче пакетов данных;
- д) соглашения в отношении передачи на хранение исходных пакетов данных;
- е) стандарты в отношении курьерской службы;
- ж) ответственность и обязательства в случае инцидентов информационной безопасности, например в случае потери данных;
- з) использование согласованной системы маркировки для критической или чувствительной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понято и что информация будет соответственно защищена;
- и) право собственности и обязанности по защите данных, соблюдение авторских прав, соответствие лицензии на программное обеспечение и аналогичные требования;
- к) технические стандарты в отношении записи и считывания информации и программного обеспечения;
- л) любые специальные меры и средства контроля и управления, которые могут потребоваться для защиты чувствительных элементов, например криптографических ключей.

Необходимо создавать и поддерживать политики, процедуры и стандарты в отношении защиты информации и физических носителей информации при их пересылке, а в соглашении по обмену следует делать на них ссылку.

Содержание любого соглашения в части безопасности должно отражать чувствительность затрагиваемой информации служебной деятельности.

Соглашения могут существовать в электронном или физическом виде и могут иметь форму официальных договоров или условий найма. В отношении чувствительной информации, определенные механизмы, используемые для обмена такой информацией, должны быть единообразны для всех органов внутренних дел и типов соглашений.



7.8.3. Физические носители информации при транспортировке

Носители информации должны быть защищены от неавторизованного доступа, неправильного использования или повреждения во время их транспортировки за пределами органа внутренних дел.

Для защиты носителей информации, передаваемых между различными пунктами назначения, необходимо учитывать следующие рекомендации:

- а) необходимо пользоваться услугами надежных перевозчиков или курьеров;
- б) список авторизованных курьеров необходимо согласовывать с руководством;
- в) необходимо разработать процедуры для проверки идентификации курьеров;
- г) упаковка должна быть достаточно прочной для защиты от любого физического повреждения, которое, вероятно, может иметь место при транспортировке, и соответствовать любым требованиям изготовителей (например программного обеспечения), необходимо обеспечивать защиту от воздействия любых факторов окружающей среды, которые могут снизить эффективность восстановления, таких как тепловой эффект, влажность или электромагнитные поля;
- д) меры и средства контроля и управления следует применять, где это необходимо, для защиты чувствительной информации от неавторизованного раскрытия или модификации, например:
 - использование запечатанных контейнеров;

- личная доставка;
- использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);
- в исключительных случаях, разбивка отправления на несколько частей, пересылаемых различными маршрутами.

Информация может быть уязвимой вследствие неавторизованного доступа, неправильного использования или искажения во время физической транспортировки, например при пересылке носителей информации по почте или через курьера.



7.8.4. Электронный обмен сообщениями

Необходимо должным образом защищать информацию, включаемую в электронный обмен сообщениями.

В отношении электронного обмена сообщениями, необходимо учитывать следующие вопросы, связанные с обеспечением безопасности:

- а) защита сообщений от неавторизованного доступа, модификации или отказа в обслуживании;
- б) обеспечение правильной адресации и передачи сообщения;
- в) общая надежность и доступность услуг;
- г) законодательные вопросы, например требования в отношении использования электронных подписей;
- д) получение одобрения до использования внешних общедоступных услуг, таких как мгновенный обмен сообщениями или разделение файлов;
- е) строгие уровни аутентификации управления доступом со стороны общедоступных сетей.

Электронный обмен сообщениями, например электронная почта, обмен данными в электронном виде и мгновенный обмен сообщениями, играет все более важную роль в коммуникациях служебной деятельности. Риски, связанные с электронным обменом сообщениями, отличаются от рисков, присущих передаче сообщений на бумаге.



7.8.5. Информационные системы служебной деятельности

Необходимо разработать и внедрить политики и процедуры защиты информации, связанной с взаимодействием информационных систем служебной деятельности.

Необходимо учитывать последствия от взаимодействия информационных систем для безопасности и служебной деятельности в целом, такие как:

а) известная уязвимость, присущая административным системам и системам учета и отчетности, где информация разделяется между различными частями органа внутренних дел;

б) уязвимость информации в системах связи служебной деятельности, например записи телефонных разговоров или переговоров по конференц-связи, конфиденциальность звонков, хранение факсов, вскрытие и рассылка электронных сообщений;

в) политика и соответствующие меры и средства контроля и управления для управления совместным использованием информации;

г) запрет на использование чувствительной информации служебной деятельности и не подлежащих оглашению документов, если данные системы не обеспечивают соответствующий уровень защиты;

д) ограничение доступа к данным личных ежедневников отдельных сотрудников, например работающих над чувствительными проектами;

е) определение категорий тех сотрудников, подрядчиков или деловых партнеров, которым разрешено использовать систему, и точек, с которых может осуществляться доступ к ней;

ж) ограничение отдельных возможностей системы для определенных категорий пользователей;

з) определение статуса пользователей, например сотрудников органа внутренних дел или подрядчиков, в отдельных директориях, для удобства других пользователей;

и) сохранение и резервное копирование информации, содержащейся в системе;

к) условия перехода на аварийный режим работы и перечень соответствующих мероприятий.

Офисные информационные системы обеспечивают возможность быстрого распространения и совместного использования информации служебной деятельности и представляют собой комбинацию документов, компьютеров, переносных компьютеров, мобильных средств связи, почты, голосовой почты, речевой связи, мультимедийных систем, услуг доставки почтовых отправок и факсов.



7.9. Мониторинг

Цель: Обнаружение неавторизованных действий, связанных с обработкой информации.

Системы должны контролироваться и события информационной безопасности должны быть зарегистрированы. Для обеспечения уверенности в том, что проблемы информационной системы выявляются, следует вести журналы эксплуатации и регистрировать неисправности.

Орган внутренних дел должен выполнять все действующие правовые требования, применимые к ее деятельности, связанной с мониторингом и регистрацией.

Мониторинг систем следует проводить с целью проверки эффективности применяемых мер и средств контроля и управления, а также подтверждения следования модели политики доступа.

7.9.1. Контрольная регистрация

Необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом.

Контрольные журналы должны включать, при необходимости:

- а) идентификаторы пользователей;
- б) даты, время и детали ключевых событий, например начало сеанса и завершение сеанса;
- в) идентичность и местоположение терминала, если это возможно;

- г) регистрацию успешных и отклоненных попыток доступа к системе;
- д) регистрацию успешных и отклоненных попыток доступа к данным или другим ресурсам;
- е) изменения конфигурации системы;
- ж) использование привилегий;
- з) использование системных утилит и прикладных программ;
- и) файлы, к которым был осуществлен доступ, и вид доступа;
- к) сетевые адреса и протоколы;
- л) сигналы тревоги, подаваемые системой управления доступом;
- м) активация и деактивация систем защиты, например антивирусных систем и систем обнаружения вторжения.

Контрольные журналы могут содержать данные о вторжениях. Необходимо принимать соответствующие меры для защиты приватности. Где возможно, системным администраторам следует запрещать стирать или деактивировать журналы регистрации их собственных действий.



7.9.2. Использование системы мониторинга

Необходимо создать процедуры для проведения мониторинга использования средств обработки информации и регулярно анализировать результаты деятельности, связанной с мониторингом.

Уровень мониторинга, необходимый для отдельных средств, следует определять с помощью оценки риска. Орган внутренних дел должен выполнять все действующие законодательные требования, применимые к ее деятельности, связанные с мониторингом. Необходимо рассмотреть следующие аспекты:

- а) авторизованный доступ, включая детали, такие как:
 - идентификаторы пользователей;
 - дату и время основных событий;
 - типы событий;
 - файлы, к которым был осуществлен доступ;
 - используемые программы/утилиты;
- б) все привилегированные действия, такие как:

- использование привилегированных учетных записей, например супервизора, привилегированного пользователя, администратора;

- запуск и остановка системы;

- подсоединение/отсоединение устройства ввода/вывода;

- в) попытки неавторизованного доступа, такие как:

- неудавшиеся или отклоненные действия пользователей;

- неудавшиеся или отклоненные действия, затрагивающие данные или другие ресурсы;

- нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;

- предупреждения от собственных систем обнаружения вторжения;

- г) предупреждения или отказы системы, такие как:

- предупреждения или сообщения пульта управления;

- изъятие системного журнала;

- предупредительные сигналы, связанные с управлением сетью;

- предупредительные сигналы, подаваемые системой управления доступом;

- д) изменения или попытки изменить параметры настройки системы безопасности и мер и средств контроля и управления.

Как часто следует анализировать результаты мониторинга деятельности, должно зависеть от возможных рисков информационной безопасности. Подлежащие рассмотрению факторы риска включают в себя:

- а) критичность процессов, которые поддерживаются прикладными программами;

- б) ценность, чувствительность и критичность затрагиваемой информации;

- в) предшествующий случай проникновения и неправильного использования системы, а также частота использования уязвимостей;

- г) степень взаимосвязи систем (особенно с общедоступными сетями);

- д) деактивацию средств регистрации.

Процедуры мониторинга использования систем нужны для обеспечения уверенности в том, что пользователи выполняют только те действия, которые были явно разрешены.

Анализ журнала регистрации способствует пониманию угроз, с которыми сталкивается система, и каким образом они могут возникать.



7.9.3. Защита информации журналов регистрации

Средства регистрации и информацию журналов регистрации следует защищать от повреждения и неавторизованного доступа.

Использование мер и средств контроля и управления должно быть нацелено на защиту от неавторизованных изменений и эксплуатационных проблем средств регистрации, включая:

- а) изменения типов записываемых сообщений;
- б) редактирование или удаление файлов журнала регистрации;
- в) превышение объема памяти носителя, содержащего файл журнала регистрации, что может приводить либо к отказу регистрировать события, либо к затиранию информации о событиях, зарегистрированных в последнюю очередь.

Архивация некоторых контрольных журналов может требоваться как часть политики хранения записей или вследствие требований собирать и хранить доказательство.

Системные журналы часто содержат большой объем информации, значительная часть которой не представляет интереса с точки зрения мониторинга безопасности. Чтобы помочь в выявлении значимых событий в целях мониторинга безопасности, необходимо рассмотреть возможность автоматической записи соответствующих типов сообщений в отдельный журнал регистраций и(или) использования подходящих системных утилит или инструментальных средств аудита для осуществления контрольного считывания и оптимизации файла.



Системные журналы необходимо защищать, так как если данные в них модифицированы или удалены, то они могут создавать ложное чувство безопасности.

7.9.4. Журналы регистрации администратора и оператора

Действия системного администратора и системного оператора следует регистрировать.

Журналы регистрации должны содержать:

а) время, когда произошло событие (успешное или неуспешное);

б) информацию о событии (например, обработанные файлы) или об отказе (например, произошла ошибка и было предпринято корректирующее действие);

в) учетную запись и имя администратора или оператора, сделавшего ее;

г) перечень задействованных процессов.

Анализ журналов регистрации системного администратора и оператора следует проводить на регулярной основе.

Система обнаружения вторжения, управление которой осуществляется вне рамок контроля системных и сетевых администраторов, может быть использована для осуществления мониторинга действий системного и сетевого администрирования на предмет соответствия.



7.9.5. Регистрация неисправностей

Неисправности следует регистрировать, анализировать, и предпринимать в их отношении необходимые действия.

Неисправности, о которых стало известно от пользователей или посредством системных программ, имеющих отношение к проблемам, связанным с системами обработки информации или коммуникационными системами, необходимо регистрировать. Должны существовать четкие правила обработки неисправностей, включая:

а) анализ журналов регистрации неисправностей для обеспечения уверенности в том, что неисправности были соответствующим образом устранены;

б) анализ корректирующих мероприятий для обеспечения уверенности в том, что меры и средства контроля и управления не были скомпрометированы и что предпринятое действие полностью авторизовано.

Должна обеспечиваться уверенность в том, что регистрация ошибок становится возможной, если данная системная функция доступна.

Регистрация ошибок и неисправностей может влиять на производительность системы. Разрешение на такую регистрацию следует давать компетентному персоналу, а уровень регистрации, требуемый для отдельных систем, должен определяться оценкой рисков, с учетом снижения производительности.



7.9.6. Синхронизация часов

Часы во всех соответствующих системах обработки информации в пределах органа внутренних дел или домена безопасности должны быть синхронизированы с установленным источником точного времени.

Если компьютер или устройство связи имеет возможность использовать часы, работающие в реальном времени, то эти часы должны быть установлены по согласованному нормативу, т. е. всемирного координированного времени или местного стандартного времени. Поскольку некоторые часы, как известно, со временем начинают «спешить» или «отставать», должна существовать процедура, которая выявляет и исправляет любые значимые отклонения.

Правильная интерпретация формата дата/время важна для обеспечения уверенности в том, что временная отметка отражает реальную дату/время. Необходимо учитывать местную специфику (например переход на «летнее время»).

Правильная установка компьютерных часов важна для обеспечения точности данных в контрольных журналах, которые могут потребоваться для расследований или в качестве доказательства в правовых (судебных) или дисциплинарных административных делах. Неаккуратные контрольные журналы могут затруднять такие расследования и дискредитировать эти доказательства. Часы, настроенные в соответствии с сигналами национальных атомных часов, передаваемыми по радио, могут использоваться как главные часы для настройки систем регистрации. Протокол сетевого времени может использоваться для поддержания всех серверов в состоянии, синхронизированном с главными часами.



8. УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ АКТИВАМ

8.1. Требования служебной деятельности по управлению доступом

Цель: Управлять доступом к информации.

Доступ к информации, средствам обработки информации и процессам служебной деятельности должен быть управляемым с учетом требований служебной деятельности и безопасности.

Правила управления доступом должны учитывать политику в отношении распространения и авторизации информации.

8.1.1. Политика управления доступом

Политика управления доступом должна создаваться, документально оформляться и пересматриваться с учетом требований служебной деятельности и безопасности для доступа.

Правила управления доступом и права каждого пользователя или группы пользователей должны быть четко сформулированы в политике управления доступом. Существует как логическое, так и физическое управление доступом, и их следует рассматривать совместно. Пользователям и поставщикам услуг должны быть представлены четко сформулированные требования служебной деятельности, предъявляемые к управлению доступом.

Необходимо, чтобы в политике было учтено следующее:

- а) требования в отношении безопасности конкретных прикладных программ служебной деятельности;
- б) определение всей информации, связанной с прикладными программами служебной деятельности, и рисков, касающихся информации;
- в) правила в отношении распространения информации и авторизации доступа, например необходимо знать принципы и уровни безопасности и классификации информации;
- г) согласованность между управлением доступом и политиками классификации информации различных систем и сетей;

д) соответствующие требования законодательства и любые договорные обязательства в отношении защиты доступа к данным или услугам;

е) стандартные профили доступа пользователей для должностных ролей в органе внутренних дел;

ж) управление прав доступа в распределенной среде или сетях с учетом всех типов доступных соединений;

з) разделение ролей в отношении управления доступом, например запрос доступа, авторизация доступа, администрирование доступа;

и) требования в отношении формального разрешения запросов доступа;

к) требования в отношении периодического пересмотра управления доступом;

л) аннулирование прав доступа.

При определении правил управления доступом следует принимать во внимание следующее:

а) различие между правилами, обязательными для исполнения, и рекомендациями, которые являются необязательными или обусловленными чем-либо;

б) установление правил, основанных на предпосылке «все в общем случае запрещено, пока явно не разрешено», а не на более слабом принципе «все в общем случае разрешено, пока явно не запрещено»;

в) изменения в информационных метках, инициированных как автоматически средствами обработки информации, так и по усмотрению пользователя;

г) изменения в правах пользователя, как устанавливаемые автоматически информационной системой, так и определенные администратором;

д) правила, которые требуют особого разрешения перед применением, а также те, которые не требуют разрешения.

Правила управления доступом должны поддерживаться формальными процедурами и четко определенными обязанностями.



8.2. Управление доступом пользователей

Цель: Обеспечить уверенность в том, что доступ предоставлен авторизованным пользователям и предотвращен неавторизованный доступ к информационным системам.

Необходимо наличие формальных процедур по контролю предоставления прав доступа к информационным системам и услугам.

Процедуры должны охватывать все стадии жизненного цикла доступа пользователей, от начальной регистрации новых пользователей до окончательной отмены регистрации пользователей, которым больше не требуется доступ к информационным системам и услугам. Особое внимание должно быть уделено, где это необходимо, контролю предоставления привилегированных прав доступа, которые позволяют пользователям изменять управление системой.

8.2.1. Регистрация пользователей

Необходима формальная процедура регистрации и снятия с учета пользователей в отношении предоставления и отмены доступа ко всем информационным системам и услугам.

Процедура управления доступом в отношении регистрации и снятия с учета пользователей должна включать:

а) использование уникальных идентификаторов пользователей, позволяющих отследить действия пользователей, чтобы они несли ответственность за свои действия; использование групповых идентификаторов следует разрешать только там, где это необходимо для служебной деятельности или по условиям эксплуатации, все это должно быть утверждено и документировано;

б) проверку того, что пользователь имеет разрешение владельца системы на использование информационной системы или услуги; наличие отдельного разрешения на право доступа от руководства также может быть уместным;

в) проверку того, что уровень предоставленного доступа соответствует целям служебной деятельности и согласуется с политикой безопасности органа внутренних дел, например не нарушает принципа разграничения обязанностей;

г) предоставление пользователям письменного заявления об их правах доступа;

д) требование от пользователей подписать заявление о принятии условий доступа;

е) обеспечение уверенности в том, что поставщики услуг не предоставляют доступ, пока процедуры авторизации не завершены;

ж) ведение формального учета всех лиц, зарегистрированных как пользователи услуг;

з) немедленную отмену или блокирование прав доступа пользователей, у которых изменились роль, или рабочее место, или уволившись из органа внутренних дел;

и) периодическую проверку и удаление или блокирование избыточных пользовательских идентификаторов и учетных записей;

к) обеспечение того, чтобы избыточные пользовательские идентификаторы не были переданы другим пользователям.

Необходимо рассмотреть возможность создания ролей доступа пользователей, основанных на требованиях служебной деятельности, которые объединяют несколько прав доступа в типовые профили доступа пользователей. Управление запросами и пересмотром предоставления прав доступа легче осуществлять на уровне таких ролей, чем на уровне отдельных прав.

Необходимо рассмотреть возможность включения положений о соответствующих санкциях в случае попыток неавторизованного доступа в трудовые договора (контракты) сотрудников и договора о предоставлении услуг.

8.2.2. Управление привилегиями

Предоставление и использование привилегий необходимо ограничивать и контролировать.

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формального процесса авторизации. Необходимо рассмотреть следующие меры:

а) определение привилегий доступа в отношении каждого системного продукта, например эксплуатируемой системы, системы управления базами данных, каждой прикладной програм-

мы и пользователей, которым эти привилегии должны быть предоставлены;

б) привилегии должны предоставляться пользователям на основании принципа необходимости и принципа «событие за событием» в соответствии с политикой управления доступом, т. е. минимального требования для их функциональной роли, только при необходимости;

в) обеспечение процесса авторизации и регистрации в отношении всех предоставленных привилегий, привилегии не должны предоставляться до завершения процесса авторизации;

г) проведение политики разработки и использования стандартных системных утилит (скриптов), для того чтобы избежать необходимости предоставления привилегий пользователям;

д) поощрение разработки и использования программ, позволяющих избежать необходимости предоставления привилегий при их исполнении;

е) использование различных идентификаторов пользователей при работе в нормальном режиме и с использованием привилегий.

Неадекватное использование привилегий в отношении администрирования системы (любой возможности или средства информационной системы, которые позволяют пользователю обходить меры и средства контроля и управления системы или прикладных программ) может быть одной из главных причин отказа или нарушения работы систем.



8.2.3. Управление паролями пользователей

Распределение паролей необходимо контролировать посредством формального процесса управления.

Процесс должен включать следующие требования:

а) пользователей необходимо обязать подписать заявление о сохранении личных паролей в тайне и сохранении групповых паролей исключительно в пределах членов данной группы; это заявление может быть включено в условия и положения занятости;

б) если пользователи самостоятельно управляют собственными паролями, им следует первоначально предоставить безопасный

временный пароль, который подлежит немедленной принудительной замене после входа в систему;

в) создание процедур проверки личности пользователя, прежде чем ему будет предоставлен новый, заменяющий или временный пароль;

г) временные пароли следует выдавать пользователям безопасным способом, при этом необходимо избегать использования третьих сторон или незащищенного (открытого) текста сообщений электронной почты;

д) временные пароли должны быть уникальны для каждого пользователя и не должны быть легко угадываемыми;

е) пользователи должны подтверждать получение паролей;

ж) пароли никогда не следует хранить в компьютерных системах в незащищенной форме;

з) пароли поставщика, установленные по умолчанию, необходимо изменить после инсталляции систем или программного обеспечения.

Пароли являются распространенным средством подтверждения личности пользователя перед предоставлением ему доступа к информационной системе или услуге в соответствии с его авторизацией. При необходимости следует рассмотреть возможность использования других технологий для идентификации и аутентификации пользователей, таких как биометрия, например проверка отпечатков пальцев, проверка подписи, а также использование аппаратных средств идентификации, например смарт-карт.



8.2.4. Пересмотр прав доступа пользователей

Руководство должно осуществлять формальный процесс периодического пересмотра прав доступа пользователей.

При пересмотре прав доступа должны учитываться следующие рекомендации:

а) права доступа должны пересматриваться регулярно, например через шесть месяцев, и после любых изменений, таких как повышение/понижение в должности, или увольнения;

б) права доступа пользователей должны пересматриваться и переназначаться при переходе с одной работы на другую в пределах одного органа внутренних дел;

в) разрешения в отношении специальных привилегированных прав доступа должны пересматриваться через небольшие интервалы времени, например через три месяца;

г) предоставленные привилегии должны пересматриваться через равные интервалы времени для обеспечения уверенности в том, что не были получены неавторизованные привилегии;

д) изменения привилегированных учетных записей должны регистрироваться для периодического анализа.

С целью поддержания эффективного контроля над доступом к данным и информационным услугам необходимо регулярно пересматривать права доступа пользователей.



8.3. Обязанности пользователя

Цель: Предотвращение неавторизованного доступа пользователей, а также компрометации или кражи информации и средств обработки информации.

Сотрудничество авторизованных пользователей - важный аспект эффективной безопасности.

Пользователи должны быть осведомлены о своих обязанностях в отношении поддержания эффективного управления доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают.

Следует внедрять политику «чистого стола» и «чистого экрана» в целях снижения риска неавторизованного доступа или повреждения бумажных документов, носителей информации и средств обработки информации.

8.3.1. Использование паролей

Пользователи должны придерживаться общепринятой практики в области безопасности при выборе и использовании паролей.

Всем пользователям следует рекомендовать:

- а) сохранять конфиденциальность паролей;
- б) избегать записи паролей (например, на бумаге, в файле программного обеспечения или карманных устройствах), если не может быть обеспечено безопасное хранение и способ хранения не утвержден;
- в) изменять пароли всякий раз, когда появляется любой признак возможной компрометации системы или пароля;
- г) выбирать качественные пароли с достаточно минимальной длиной, которые:
 - легко запомнить;
 - не подвержены угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например имен, номеров телефонов, дат рождения и т. д.;
 - не могут быть восстановлены по словарям (т. е., не содержат слов, содержащихся в словарях);
 - не содержат последовательных идентичных символов, и не состоят из полностью числовых или полностью буквенных групп;
- д) изменять пароли через разные интервалы времени или после определенного числа обращений к системе (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли) и избегать повторного или циклического использования старых паролей;
- е) изменять временные пароли при первом начале сеанса;
- ж) не включать пароли ни в какой автоматизированный процесс начала сеанса, например с использованием хранимых макрокоманд или функциональных клавиш;
- з) не использовать коллективно индивидуальные пользовательские пароли;
- и) не использовать один и тот же пароль для служебной деятельности и некоммерческих целей.

Если пользователи нуждаются в доступе к многочисленным услугам, системам или платформам и вынуждены использовать несколько разных паролей, они должны знать, что могут использовать единый качественный пароль для всех услуг при уверенности, что разумный уровень защиты для хранения пароля был создан в рамках каждой услуги, системы или платформы.

Особую осторожность следует соблюдать при управлении системы «справочного стола», имеющей дело с утерянными или забытыми паролями, поскольку это может быть средством атаки на систему паролей.



8.3.2. Оборудование пользователя, оставленное без присмотра

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра

Всем пользователям необходимо знать требования безопасности и процедуры в отношении защиты оставленного без присмотра оборудования, а также их обязанности по обеспечению такой защиты. Пользователям рекомендуется:

а) завершать активные сеансы по окончании работы, если отсутствует соответствующий механизм блокировки, например защищенная паролем экранная заставка;

б) завершить сеанс на системах мэйнфреймов, серверах и офисных персональных компьютерах, когда работа завершена (т. е. не только выключить экран персонального компьютера или терминал);

в) обеспечивать безопасность персональных компьютеров или терминалов от несанкционированного использования с помощью блокировки клавиатуры или эквивалентных средств контроля, например доступа по паролю, когда оборудование не используется.

Оборудование, установленное в пользовательских зонах, например рабочие станции или файловые серверы, может потребовать специальной защиты от несанкционированного доступа, если оно оставлено без присмотра на длительный период.



8.3.3. Политика «чистого стола» и «чистого экрана»

Необходимо принять политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации.

Политика «чистого стола» и «чистого экрана» должна учитывать классификацию информации, законодательные и договорные требования, а также соответствующие риски и корпоративную культуру органа внутренних дел. Необходимо рассмотреть следующие рекомендации:

а) носители (бумажные или электронные), содержащие чувствительную или критическую информацию служебной деятельности, когда они не используются, следует убирать и запереть (лучше всего, в несгораемый сейф или шкаф), особенно, когда помещение пусто;

б) компьютеры и терминалы, когда их оставляют без присмотра, следует выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем, токеном или аналогичным механизмом аутентификации пользователя, а также необходимо применять кодовые замки, пароли или другие меры и средства контроля и управления в то время, когда эти устройства не используются;

в) необходимо обеспечить защиту пунктов приема/отправки корреспонденции, а также автоматических факсимильных аппаратов;

г) необходимо предотвращать несанкционированное использование фотокопировальных устройств и другой воспроизводящей техники (сканеров, цифровых фотоаппаратов);

е) документы, содержащие чувствительную или критическую информацию, необходимо немедленно изымать из принтеров.

Политика «чистого стола»/«чистого экрана» снижает риски несанкционированного доступа, потери и повреждения информации как во время рабочего дня, так и вне рабочего времени. Сейфы или другие формы средств безопасного хранения также могут защищать хранимую в них информацию от форс-мажорных обстоятельств, таких как пожар, землетрясение, наводнение или взрыв.

Стоит обратить внимание на использование принтеров с функцией ПИН-кода, тогда только инициаторы отправления на печать смогут получать свои распечатки, и только если они стоят рядом с принтером.



8.4. Управление доступом к сети

Цель: Предотвратить неавторизованный доступ к сетевым услугам.

Доступ к внутренним и внешним сетевым услугам должен быть контролируемым.

Это необходимо для получения уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым услугам, не нарушают их безопасность, путем:

а) обеспечения соответствующих интерфейсов между сетью органа внутренних дел и сетями, принадлежащими другим организациям, и общедоступными сетями;

б) внедрения соответствующих механизмов аутентификации в отношении пользователей и оборудования;

в) предписанного управления доступом пользователей к информационным услугам.

8.4.1. Политика использования сетевых услуг

Пользователям следует предоставлять доступ только к тем услугам, на использование которых они были специально уполномочены.

Следует сформулировать политику относительно использования сетей и сетевых услуг.

В политике необходимо рассмотреть:

а) сети и сетевые услуги, к которым разрешен доступ;

б) процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ;

в) меры и средства контроля и управления, а также процедуры управления по защите доступа к сетевым подключениям и сетевым услугам;

г) средства, используемые для осуществления доступа к сетям и сетевым услугам (например условия, обеспечивающие возможность доступа по коммутируемой телефонной линии к провайдеру Интернет-услуг или удаленной системе).

Политика использования сетевых услуг должна быть согласована с политикой управления доступом.

Несанкционированные и незащищенные подключения к сетевым услугам могут затрагивать целый орган внутренних дел. Мера и средство контроля и управления, в частности, важна для сетевых подключений к чувствительным или критическим прикладным программам служебной деятельности, или в отношении пользователей, находящихся в зонах высокого риска, например в общественных местах или за пределами орган внутренних дел, т. е. в общественных или внешних зонах, которые находятся за пределами непосредственного управления и контроля безопасностью со стороны органа внутренних дел.



8.4.2. Аутентификация пользователей для внешних соединений

Для управления доступом удаленных пользователей следует применять соответствующие методы аутентификации.

Аутентификация удаленных пользователей может быть достигнута при использовании, например методов, основанных на применении средств криптографии, аппаратных средств защиты (токенов) или протоколов «запрос-ответ». Примером возможной реализации таких методов могут служить различные решения в отношении виртуальных частных сетей. Выделенные частные линии могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры, меры и средства контроля и управления обратного вызова, например использование модемов с обратным вызовом, могут обеспечить защиту от несанкционированных и нежелательных подключений к средствам обработки информации органа внутренних дел. Указанные меры позволяют произвести аутентификацию пользователей, пытающихся установить удаленную связь с сетью орган внутренних дел. При использовании данной меры и средства контроля и управления орган внутренних дел не следует применять сетевые сервисы, которые включают переадресацию вызова, или, если они это делают, то они должны отключить использование таких функций, чтобы избежать недостатков, связанных с переадресацией вызова. Процесс обратного вызова должен обеспечить уверенность в том, что фактическое

разъединение происходит на стороне орган внутренних дел. В противном случае, удаленный пользователь может держать линию открытой, считая, что произошла проверка обратного вызова. Процедуры, меры и средства контроля и управления обратного вызова следует тщательно протестировать на предмет наличия такой возможности.

Аутентификация узла может служить альтернативным средством аутентификации групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования. Для аутентификации узла могут применяться криптографические методы, основанные, например, на механизме сертификации. Это является частью некоторых решений, основанных на виртуальных частных сетях.

Должны быть реализованы дополнительные меры и средства контроля и управления аутентификацией для управления доступом к беспроводным сетям. В частности, необходимо проявлять особую осторожность при выборе мер и средств контроля и управления для беспроводных сетей по причине больших возможностей необнаруживаемого перехвата и ввода сетевого трафика.

Внешние соединения обеспечивают благоприятную возможность для несанкционированного доступа к информации служебной деятельности, например доступа с использованием методов соединения по телефонной линии. Существуют различные методы аутентификации, некоторые из которых обеспечивают больший уровень защиты, чем другие, например методы, основанные на использовании средств криптографии, могут обеспечить достаточно надежную защиту. Исходя из оценки риска, важно определить требуемый уровень защиты. Это необходимо для соответствующего выбора метода аутентификации.

Наличие возможности автоматического подсоединения к удаленному компьютеру – это один из способов получения несанкционированного доступа к прикладной программе служебной деятельности. Это особенно важно, если для подсоединения используется сеть, которая находится вне сферы контроля управления безопасностью органа внутренних дел.



8.4.3. Идентификация оборудования в сетях

Автоматическую идентификацию оборудования необходимо рассматривать как средство для аутентификации соединений, осуществляемых с определенных мест или определенного оборудования.

Идентификацию оборудования можно применять в тех случаях, когда важно, чтобы связь могла быть инициирована только с определенного места или оборудования. Для того чтобы показать, разрешено ли этому оборудованию подсоединение к сети, может быть использован внутренний или прикрепленный к оборудованию идентификатор. Такие идентификаторы должны четко показывать, к какой сети разрешено подключать оборудование, если эта сеть не единственная и, особенно, если эти сети имеют разную степень чувствительности. Для обеспечения безопасности идентификатора оборудования может возникнуть необходимость физической защиты оборудования.

Эти меры и средства контроля и управления могут быть дополнены другими методами, направленными на аутентификацию пользователя оборудования. Идентификация оборудования может применяться дополнительно к аутентификации пользователя.



8.4.4. Защита портов дистанционной диагностики и конфигурации

Физический и логический доступ для портов дистанционной диагностики и конфигурации должен быть контролируемым и управляемым.

Возможные меры и средства контроля и управления доступом к портам дистанционной диагностики и конфигурации включают в себя использование блокировки клавиш и поддерживающих процедур для контроля физического доступа к порту. Примером такой поддерживающей процедуры является обеспечение уверенности в том, что доступ к портам дистанционной диагностики и конфигурации осуществляется только при условии взаимной договоренности между руководителем, отвечающим за

предоставление компьютерных услуг, и персоналом по поддержке аппаратных/программных средств.

Порты, сервисы и аналогичные средства, установленные на компьютере или сетевом оборудовании, которые определенно не требуются для функциональности служебной деятельности, следует блокировать или удалять.

Многие компьютерные системы, сетевые системы и системы связи внедряются со средствами удаленной диагностики или конфигурации для использования инженерами по обслуживанию. Будучи незащищенными, эти диагностические порты предоставляют возможность неавторизованного доступа.



8.4.5. Разделение в сетях

Группы информационных услуг, пользователей и информационных систем в пределах сети должны быть разделены.

Один из методов контроля безопасности больших сетей состоит в том, чтобы разделить их на отдельные логические сетевые домены, например на внутренние сетевые домены органа внутренних дел и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Совокупность последовательных мер и средств контроля и управления может быть применена в различных логических сетевых доменах для дальнейшего разделения среды сетевой безопасности, например общедоступные системы, внутренние сети и критические активы. Домены должны определяться на основе оценки риска и различных требований в отношении безопасности в пределах каждого из доменов.

Такой сетевой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для управления доступом и информационным потоком между двумя доменами. Данный шлюз следует конфигурировать для фильтрации трафика между доменами и для блокирования несанкционированного доступа в соответствии с политикой органа внутренних дел по управлению доступом. Примером шлюза такого типа является межсетевой экран. Другим методом разделения отдельных логических доменов является ограничение сете-

вого доступа при использовании виртуальных частных сетей для групп пользователей в пределах органа внутренних дел.

Сети также могут быть разделены с помощью функциональных возможностей сетевых устройств, например IP-коммутации. Отдельные домены могут быть, кроме того, реализованы посредством управления потоками сетевых данных при использовании возможностей маршрутизации/коммутации, например списков управления доступом.

Критерии для разделения сетей на домены следует основывать на политике управления доступом и требованиях к доступу с учетом влияния на относительную стоимость и производительность включения соответствующей технологии маршрутизации сетей и шлюзов.

Кроме того, разделение сетей должно основываться на ценности и классификации информации, хранимой или обрабатываемой в сети, уровнях доверия или сферах деятельности, для того чтобы снизить последствия от прерывания услуг.

Следует уделять внимание отделению беспроводных сетей от внутренних и частных сетей. Поскольку периметры беспроводных сетей не являются достаточно определенными, следует проводить оценку риска, чтобы идентифицировать меры и средства контроля и управления (например, строгую аутентификацию, криптографические методы и выбор частоты) для поддержки разделения сетей.

Сети все более распространяются за традиционные границы органа внутренних дел, поскольку создаются деловые партнерства, которые могут потребовать коммуникаций или совместного использования сетевой инфраструктуры и средств обработки информации. Такие расширения могут увеличить риск несанкционированного доступа к существующим информационным системам, которые используют сеть, причем в отношении некоторых из этих систем, вследствие их чувствительности или критичности, может потребоваться защита от других пользователей, получивших доступ к сети.



8.4.6. Управление сетевыми соединениями

Присоединение пользователей к совместно используемым сетям, особенно тем, которые выходят за рамки органа внутренних дел, необходимо ограничивать в соответствии с политикой управления доступом и требованиями прикладных программ служебной деятельности.

Права пользователей в отношении сетевого доступа должны поддерживаться и обновляться в соответствии с требованиями политики управления доступом.

Возможность подсоединения пользователей может ограничиваться сетевыми шлюзами, фильтрующими трафик посредством предварительно определенных таблиц или правил. Примерами прикладных программ, к которым следует применить ограничения являются:

- а) обмен сообщениями, например электронная почта;
- б) передача файлов;
- в) интерактивный доступ;
- г) доступ к прикладной программе.

Следует рассмотреть права доступа к сети, приуроченные к определенному времени суток или дате.

Требования политики управления доступом для совместно используемых сетей, особенно тех, которые выходят за рамки органа внутренних дел, могут вызвать необходимость внедрения дополнительных мер и средств контроля и управления, чтобы ограничить возможности пользователей по подсоединению.



8.4.7. Управление сетевой маршрутизацией

Для сетей следует внедрять меры и средства контроля и управления маршрутизацией, чтобы обеспечить уверенность в том, что подсоединения компьютеров и информационные потоки не нарушают политику управления доступом к прикладным программам служебной деятельности.

Необходимо, чтобы меры и средства контроля и управления маршрутизацией основывались на механизмах проверки реальных адресов источника и получателя.

Шлюзы безопасности могут использоваться для подтверждения адресов источника и получателя на внутренней и внешней точках управления сетью, если используются технологии трансляции сетевых адресов и (или) прокси-сервер. Необходимо, чтобы специалисты, занимающиеся внедрением, были осведомлены о преимуществах и недостатках различных используемых механизмов. Требования в отношении мер и средств контроля и управления маршрутизацией сети должны основываться на политике управления доступом.

Сети совместного использования, особенно те, которые выходят за рамки органа внутренних дел, могут потребовать внедрения дополнительных мер и средств контроля и управления маршрутизацией. Это, особенно, касается сетей, используемых совместно с пользователями третьей стороны.



8.5. Управление доступом к эксплуатируемой системе

Цель: Предотвратить несанкционированный доступ к эксплуатируемым системам.

Средства безопасности следует использовать, для того чтобы возможность осуществления доступа предоставлялась только авторизованным пользователям. Необходимо, чтобы данные средства могли обеспечить следующее:

- а) аутентификацию авторизованных пользователей в соответствии с определенной политикой управления доступом;
- б) регистрацию успешных и неудавшихся попыток аутентификации для осуществления доступа к системе;
- в) регистрацию использования специальных системных привилегий;
- г) срабатывание сигнализации при нарушении политик безопасности системы;
- д) обеспечение соответствующих средств для аутентификации;
- е) при необходимости, ограничение времени подсоединения пользователей.

8.5.1. Безопасные процедуры начала сеанса

Доступ к эксплуатируемым системам должен контролироваться посредством безопасной процедуры начала сеанса.

Процедура регистрации в эксплуатируемой системе должна быть спроектирована так, чтобы свести к минимуму возможность несанкционированного доступа. Поэтому необходимо, чтобы процедура начала сеанса раскрывала минимум информации о системе, во избежание оказания какой-либо ненужной помощи неавторизованному пользователю. Правильная процедура начала сеанса характеризуется следующими свойствами:

а) не отображает наименований системы или прикладных программ, пока процесс начала сеанса не будет успешно завершен;
б) отображает общее предупреждение о том, что доступ к компьютеру могут получить только авторизованные пользователи;
в) не предоставляет сообщений-подсказок в течение процедуры начала сеанса, которые могли бы помочь неавторизованному пользователю;

г) подтверждает информацию начала сеанса только по завершении ввода всех исходных данных, в случае ошибочного ввода, система не должна показывать, какая часть данных является правильной или неправильной;

д) ограничивает число разрешенных неудачных попыток начала сеанса (например три попытки) и предусматривает:

- протоколирование неудачных и удачных попыток;
- включение временной задержки прежде, чем будут разрешены дальнейшие попытки начала сеанса, или отклонение любых дальнейших попыток без специальной авторизации;
- разъединение сеанса связи и передачи данных;
- отправление предупредительного сообщения на системный пульт, если достигнуто максимальное число попыток начала сеанса;
- установление числа повторного ввода паролей с учетом минимальной длины пароля и значимости защищаемой системы;

е) ограничивает максимальное и минимальное время, разрешенное для процедуры начала сеанса, если оно превышено, система должна прекратить начало сеанса;

ж) отображает следующую информацию в отношении успешного завершения начала сеанса:

- дату и время предыдущего успешного начала сеанса;
- подробную информацию о любых неудачных попытках начала сеанса, начиная с последнего успешного начала сеанса;
- з) не отображает введенный пароль или предусматривает скрытие знаков пароля с помощью символов;
- и) не передает пароли открытым текстом по сети.

8.5.2. Идентификация и аутентификация пользователя

Необходимо, чтобы все пользователи имели уникальный идентификатор (идентификатор пользователя), предназначенный только для их личного использования, и должен быть выбран подходящий способ проверки для подтверждения заявленной подлинности пользователя.

Меры и средства контроля и управления должна применяться в отношении всех типов пользователей (включая персонал технической поддержки, операторов, администраторов сети, системных программистов и администраторов баз данных).

Идентификаторы пользователей необходимо использовать для отслеживания действий подотчетного лица. Регулярные действия пользователей не должны выполняться из привилегированных учетных записей.

При исключительных обстоятельствах, когда имеется очевидная выгода для служебной деятельности, может использоваться общий идентификатор для группы пользователей или для выполнения определенной работы. В таких случаях необходимо документально оформлять разрешение руководства. Могут потребоваться дополнительные меры и средства контроля и управления для поддержания отслеживаемости.

Разрешение на индивидуальное использование группового идентификатора следует давать только тогда, когда функции общедоступны, или нет необходимости отслеживать действия, выполняемые с помощью данного идентификатора (например доступ только для чтения), или когда применяются другие меры контроля (например пароль для группового идентификатора выдается единовременно только для одного сотрудника и такой случай регистрируется).

Там, где требуются надежная аутентификация и идентификация личности, следует использовать аутентификационные методы, альтернативные по отношению к паролям, такие как криптографические средства, смарт-карты, токены или биометрические средства.

Пароли являются очень распространенным способом обеспечения идентификации и аутентификации, основанном на тайне, которую знает только пользователь. Того же результата можно достигнуть средствами криптографии и аутентификационными протоколами. Надежность идентификации и аутентификации пользователя должна соответствовать чувствительности информации, к которой нужно осуществлять доступ.

Такие объекты как токены с памятью или смарт-карты, которыми обладают пользователи, также могут применяться для идентификации и аутентификации. Биометрические технологии аутентификации, которые используют уникальные характеристики или особенности индивидуума, также могут служить для подтверждения подлинности личности. Сочетание различных технологий и механизмов, связанных безопасным способом, обеспечивает более надежную аутентификацию.



8.5.3. Система управления паролями

Системы управления паролями должны быть интерактивными и должны обеспечивать уверенность в качестве паролей.

Рекомендация по реализации

Система управления паролями должна:

- а) предписывать использование индивидуальных пользовательских идентификаторов и паролей с целью установления персональной ответственности;
- б) позволять пользователям выбирать и изменять свои пароли, и включать процедуру подтверждения ошибок ввода;
- в) предписывать использование качественных паролей;
- г) принуждать к изменению паролей;

- д) заставлять пользователей изменять временные пароли при первом начале сеанса;
- е) вести учет предыдущих пользовательских паролей и предотвращать их повторное использование;
- ж) не отображать пароли на экране при их вводе;
- з) хранить файлы паролей отдельно от данных прикладных систем;
- и) хранить и передавать пароли в защищенной (например, зашифрованной или хешированной) форме.

8.5.4. Использование системных утилит

Использование утилит, которые могли бы обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ, следует ограничивать и строго контролировать.

Необходимо рассмотреть следующие рекомендации по использованию системных утилит:

- а) использование процедур идентификации, аутентификации и авторизации для системных утилит;
- б) отделение системных утилит от прикладных программ;
- в) ограничение использования системных утилит минимальным числом доверенных авторизованных пользователей;
- г) авторизация на использование специальных системных утилит;
- д) ограничение доступности системных утилит, например на время внесения авторизованных изменений;
- е) регистрация использования всех системных утилит;
- ж) определение и документальное оформление уровней авторизации в отношении системных утилит;
- з) удаление или блокирование ненужного программного обеспечения утилит и системного программного обеспечения;
- и) обеспечение недоступности системных утилит для пользователей, имеющих доступ к прикладным программам на системах, где требуется разделение обязанностей.

На большинстве компьютеров, как правило, установлена одна или несколько системных обслуживающих программ (утилит), которые позволяют обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ.



8.5.5. Лимит времени сеанса связи

Неактивные сеансы должны быть закрыты после определенного периода бездействия.

Необходимо, чтобы механизм блокировки по времени обеспечивал очистку окна сеанса, а также, возможно позднее, после определенного периода бездействия закрывал прикладную программу и сетевые сеансы. Задержка, связанная с блокировкой по времени, должна отражать риски безопасности этой области, классификацию обрабатываемой информации и используемых прикладных программ, а также риски, связанные с пользователями оборудования.

Для некоторых систем может быть предусмотрена ограниченная форма средств блокировки по времени, которая очищает экран и предотвращает неавторизованный доступ, но не закрывает прикладные программы или сетевые сеансы.

Данная мера и средство контроля и управления особенно важна в местах повышенного риска, например в общедоступных местах или на внешней территории, находящейся вне сферы действия управления безопасностью органа внутренних дел. Для предотвращения доступа неавторизованных лиц и атак типа «отказ в обслуживании» сеансы необходимо закрывать.



8.5.6. Ограничения времени соединения

Ограничения на время соединения должны быть использованы для обеспечения дополнительной безопасности прикладных программ с высокой степенью риска.

Необходимо рассмотреть меры и средства контроля и управления в отношении времени подсоединения для чувствительных компьютерных приложений, особенно в местах повы-

шенного риска, например общедоступных местах или на внешней территории, находящейся вне сферы действия управления безопасности органа внутренних дел. Примерами таких ограничений являются:

а) использование заранее определенных отрезков времени, например для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;

б) ограничение времени подключения нормальными часами работы органа внутренних дел, если нет необходимости в сверхурочной или более продолжительной работе;

в) проведение повторной аутентификации через запланированные интервалы времени.

Ограничение периода, в течение которого разрешены подсоединения к компьютерным сервисам, уменьшает интервал времени, в течение которого существует риск неавторизованного доступа. Ограничение продолжительности активных сеансов не позволяет пользователям держать сеансы открытыми, чтобы предотвратить повторную аутентификацию.



8.6. Управление доступом к информации и прикладным программам

Цель: Предотвратить неавторизованный доступ к информации прикладных систем.

Необходимо использовать средства безопасности для ограничения доступа к прикладным системам и внутри данных систем.

Круг лиц, имеющих логический доступ к прикладному программному обеспечению и информации, должен быть ограничен только авторизованными пользователями. Необходимо, чтобы прикладные системы обеспечивали следующее:

а) управление доступом пользователей к информации и функциям прикладных систем в соответствии с определенной политикой управления доступом;

б) защиту от неавторизованного доступа любой утилиты, программного обеспечения эксплуатируемой системы и вредоносной программы, которые позволяют отменять или обходить

меры и средства контроля и управления системы или прикладных программ;

в) не представляли угрозу безопасности другим системам, совместно с которыми используются информационные ресурсы.

8.6.1. Ограничение доступа к информации

Доступ пользователей и персонала поддержки к информации и функциям прикладных систем должен ограничиваться в соответствии с определенной политикой в отношении управления доступом.

Ограничения доступа должны основываться на требованиях в отношении отдельных прикладных программ служебной деятельности. Политика управления доступом должна соответствовать политике доступа органа внутренних дел.

Необходимо рассмотреть возможность применения следующих рекомендаций для соблюдения требований по ограничению доступа:

а) наличие пунктов меню, позволяющих управлять доступом к функциям прикладных систем;

б) управление правами доступа пользователей, например чтение, запись, удаление, выполнение;

в) управление правами доступа других прикладных программ;

г) обеспечение уверенности в том, что данные, выводимые из прикладных систем, обрабатывающих чувствительную информацию, содержат только требуемую информацию и отправлены только в адреса авторизованных терминалов и мест назначения; необходим периодический анализ процесса вывода для обеспечения уверенности в том, что избыточная информация удалена.

8.6.2. Изоляция чувствительных систем

Чувствительные системы должны иметь специализированную (изолированную) вычислительную среду.

В отношении систем, обрабатывающих чувствительную информацию, необходимо рассмотреть следующее:

а) владелец прикладной программы должен определить и документально оформить степень чувствительности данной прикладной программы;

б) если чувствительная прикладная программа должна работать в среде совместного использования, владельцем данной прикладной программы должны быть выявлены другие прикладные программы, с которыми будут совместно использоваться ресурсы, а также идентифицированы и приняты соответствующие риски.

Некоторые прикладные программы системы достаточно чувствительны к потенциальному ущербу и поэтому требуют особой эксплуатации. Чувствительность может указывать, что прикладная программа системы:

а) должна работать на выделенном компьютере;

б) должна разделять ресурсы только с доверенными прикладными программами системы.

Изоляция может быть достигнута при использовании физических или логических методов.



8.7. Мобильная вычислительная техника и дистанционная работа

Цель: Обеспечить уверенность в информационной безопасности при использовании средств мобильной вычислительной техники и дистанционной работы.

Следует соизмерять требуемую защиту со специфичными рисками работы в удаленном режиме. При использовании мобильной вычислительной техники следует учитывать риски, связанные с работой в незащищенной среде, и применять соответствующие средства защиты. В случаях дистанционной работы органу внутренних дел следует предусмотреть защиту мест дистанционной работы и обеспечить уверенность в соответствующей организации подобного способа работы.

8.7.1. Мобильная вычислительная техника и связь

Необходимо принять формальную политику и обеспечить соответствующие меры безопасности для защиты от рисков, связанных с работой со средствами мобильной вычислительной техники и связи.

При использовании мобильных вычислительных средств и средств связи, например ноутбуков, карманных компьютеров, лэптопов, смарт-карт и мобильных телефонов, необходимо принимать специальные меры для обеспечения уверенности в том, что служебная информация не скомпрометирована. Политика использования мобильных вычислительных средств должна учитывать риски, связанные с работой с переносными устройствами в незащищенной среде.

Политика использования мобильных вычислительных средств должна включать требования к физической защите, управлению доступом, использованию средств криптографии, резервирования и защиты от вирусов. Такая политика должна также включать правила и рекомендации относительно подсоединения мобильных средств к сетям, а также руководство по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных вычислительных средств в общедоступных местах, конференц-залах и других незащищенных местах вне органа внутренних дел. Необходимо обеспечить защиту от неавторизованного доступа или раскрытия информации, хранимой и обрабатываемой этими средствами, например с помощью средств криптографии.

Важно при использовании мобильных вычислительных средств в общедоступных местах проявлять осторожность, во избежание риска вмешательства неавторизованных лиц. Необходимо внедрить и поддерживать в актуальном состоянии процедуры защиты от вредоносной программы.

Необходимо регулярно делать резервные копии критической информации, используемой в служебной деятельности. Следует также обеспечить доступность оборудования для быстрого и удобного резервного копирования информации. В отношении ре-

зервных копий необходимо обеспечить адекватную защиту, например от кражи или потери информации.

Соответствующую защиту необходимо обеспечить в отношении использования мобильных средств, подсоединенных к сетям. Удаленный доступ к информации служебной деятельности через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при условии внедрения соответствующих механизмов управления доступом.

Мобильные вычислительные средства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра/забывают, например в автомобилях или других видах транспорта, гостиничных номерах, конференц-центрах и местах встреч. Для случаев потери или кражи мобильных вычислительных средств должна быть установлена специальная процедура, учитывающая требования безопасности органа внутренних дел. Оборудование, в котором переносится важная, чувствительная и (или) критическая информация служебной деятельности, не следует оставлять без присмотра и по возможности должно быть физически заблокировано или должны быть использованы специальные замки для обеспечения безопасности оборудования.

Необходимо провести тренинг сотрудников, использующих мобильные вычислительные средства, с целью повышения осведомленности о дополнительных рисках, связанных с таким способом работы и мерах и средствах контроля и управления, которые должны быть выполнены.

Беспроводные подсоединения к сети мобильной связи аналогичны другим типам подсоединения к сети, однако они имеют важные отличия, которые необходимо учитывать при определении мер и средств контроля и управления. Типичными отличиями являются:

а) некоторые беспроводные небезупречные протоколы безопасности;

б) невозможность резервного копирования информации в мобильных вычислительных средствах вследствие ограниченной пропускной способности сети и (или) из-за того, что переносное оборудование не может быть подсоединено на время, которое запланировано для резервирования.



8.7.2. Дистанционная работа

Политика, планы и процедуры эксплуатации должны быть разработаны и внедрены для дистанционной работы.

Органы внутренних дел должны разрешать дистанционную работу только при уверенности в том, что применяются соответствующие соглашения о безопасности и меры и средства контроля и управления, которые, в свою очередь, согласуются с политикой безопасности органа внутренних дел.

Следует обеспечить необходимую защиту места дистанционной работы в отношении, например хищения оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам орган внутренних дел или неправильного использования оборудования. Дистанционная работа должна быть санкционирована и контролируема руководством, и должна быть обеспечена уверенность в том, что имеются соответствующие меры для данного способа работы.

Необходимо принимать во внимание следующее:

а) существующую физическую безопасность места дистанционной работы, включая физическую безопасность здания и окружающей среды;

б) предлагаемые условия дистанционной работы;

в) требования в отношении безопасности коммуникаций, учитывая потребность в удаленном доступе к внутренним системам органа внутренних дел, чувствительность информации, к которой будет осуществляться доступ и которая будет передаваться по каналам связи, а также чувствительность самих внутренних систем;

г) угрозу несанкционированного доступа к информации или ресурсам со стороны других лиц, использующих место дистанционной работы, например членов семьи и друзей;

д) использование домашних компьютерных сетей, а также требования или ограничения в отношении конфигурации услуг беспроводных сетей;

е) политики и процедуры для предотвращения споров, касающихся прав на интеллектуальную собственность, разработанную на оборудовании, находящемся в частной собственности;

ж) доступ к оборудованию, находящемуся в частной собственности (для проверки безопасности машины или во время проведения расследований), который может быть запрещен законодательством;

з) лицензионные соглашения в отношении программного обеспечения, которые таковы, что орган внутренних дел может стать ответственной за лицензирование клиентского программного обеспечения на рабочих станциях, находящихся в частной собственности сотрудников, подрядчиков или пользователей третьей стороны;

и) требования в отношении антивирусной защиты и межсетевых экранов.

Рекомендации и необходимые организационные меры включают, в частности:

а) обеспечение подходящим оборудованием и мебелью для дистанционной работы в тех случаях, когда запрещается использование оборудования, находящегося в частной собственности, если оно не находится под контролем орган внутренних дел;

б) определение видов разрешенной работы, времени работы, классификацию информации, которая может поддерживаться внутренними системами и услугами, к которым разрешен доступ сотруднику в дистанционном режиме;

в) обеспечение подходящим телекоммуникационным оборудованием, включая методы обеспечения безопасности удаленного доступа;

г) физическую безопасность;

д) правила и рекомендации в отношении доступа членов семьи и друзей к оборудованию и информации;

е) обеспечение технической поддержки и обслуживания аппаратного и программного обеспечения;

ж) процедуры в отношении резервного копирования данных и обеспечения непрерывности служебной деятельности;

з) аудит и мониторинг безопасности;

и) аннулирование полномочий, отмену прав доступа и возвращение оборудования в случае прекращения работы в дистанционном режиме.

9. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ ПРИОБРЕТЕНИИ, РАЗРАБОТКЕ И ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

9.1. Требования безопасности информационных систем

Цель: Обеспечить уверенность в том, что безопасность является неотъемлемой частью информационных систем.

Информационные системы включают эксплуатируемые системы, инфраструктуру, прикладные программы служебной деятельности, готовые продукты, услуги и прикладные программы, разработанные пользователями. Проектирование и внедрение информационной системы, поддерживающей процесс служебной деятельности, может быть критичным с точки зрения безопасности. Требования безопасности следует выявлять и согласовывать до разработки и (или) внедрения информационных систем.

Все требования безопасности следует выявлять на стадии определения задач проекта, а также обосновывать, согласовывать и документально оформлять в рамках общего проекта по внедрению информационной системы.

9.1.1. Анализ требований безопасности и спецификация

Необходимо, чтобы в формулировках требований служебной деятельности для новых информационных систем или при модернизации существующих информационных систем были определены требования к мерам и средствам контроля и управления безопасностью.

В спецификациях требований к мерам и средствам контроля и управления следует учитывать как встроенные в информационную систему автоматизированные меры и средства контроля и управления, так и необходимость поддержки ручного управления. Аналогично следует подходить к оценке пакетов прикладных программ, разработанных или приобретенных для прикладных программ служебной деятельности.

Необходимо, чтобы требования безопасности и соответствующие меры и средства контроля и управления отражали цен-

ность информационных активов и потенциальный ущерб служебной деятельности, который мог бы явиться результатом недостаточности мер безопасности или их отсутствия.

Системные требования в отношении информационной безопасности и процессов реализации безопасности необходимо включать на ранних стадиях проектов, касающихся информационных систем. Определение мер и средств контроля и управления на стадии проектирования системы позволяет существенно снизить затраты на их внедрение и поддержку по сравнению с разработкой мер и средств контроля и управления во время или после внедрения системы.

В случае приобретения готовых продуктов необходимо соблюдение формального процесса приобретения и тестирования. В договорах с поставщиками должны учитываться определенные требования безопасности. Если функциональность безопасности в предлагаемом готовом продукте не удовлетворяет установленному органом внутренних дел требованию, то тогда необходимо повторно рассмотреть порождаемый этим фактом риск и связанные с ним меры и средства контроля и управления прежде, чем продукт будет приобретен. Если обеспечивается дополнительная функциональность, и это создает риск безопасности, то ее следует блокировать, или пересмотреть предлагаемую структуру управления, чтобы определить возможность использования преимуществ имеющейся дополнительной функциональности.

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 [19] содержит рекомендации по использованию процессов управления риском для определения требований к мерам и средствам контроля и управления безопасностью. !

9.2. Корректная обработка в прикладных программах

Цель: Предотвратить ошибки, потерю, неавторизованную модификацию или нецелевое использование информации в прикладных программах.

Соответствующие меры и средства контроля и управления необходимо предусмотреть в прикладных программах, включая прикладные программы, разработанные пользователем, для обеспечения уверенности в корректности обработки данных. Указан-

ные меры и средства контроля и управления должны также включать возможность подтверждения корректности ввода, обработки и вывода данных.

Дополнительные меры и средства контроля и управления могут потребоваться для систем, которые обрабатывают или оказывают воздействие на чувствительную, ценную или критическую информацию. Такие меры и средства контроля и управления безопасности должны быть определены на основе требований безопасности и оценки рисков.

9.2.1. Подтверждение корректности входных данных

Входные данные для прикладных программ должны проходить процедуру подтверждения с целью обеспечения уверенности в их корректности и соответствии.

Проверки следует проводить при вводе транзакций служебной деятельности, справочников (например имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (например цены продаж, курсы валют, ставки налогов). Необходимо рассмотреть следующие рекомендации:

а) двойной ввод или другие процедуры проверки ввода, например проверка границ или ограничение полей до определенных диапазонов вводимых данных с целью обнаружения следующих ошибок:

- значений, выходящих за допустимый диапазон;
- недопустимых символов в полях данных;
- отсутствующих или неполных данных;
- превышения верхних и нижних пределов объема данных;
- запрещенных или противоречивых контрольных данных;

б) периодическая проверка содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

в) сверка печатных копий вводимых документов на предмет выявления любых несанкционированных изменений (необходимо, чтобы все изменения во вводимых документах были утверждены);

г) процедуры реагирования на ошибки проверки;

д) процедуры проверки достоверности вводимых данных;

е) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;

ж) создание журнала регистрации действий, связанных с процессом ввода данных.

Там, где это целесообразно, можно рассмотреть автоматическую экспертизу и проверку вводимых данных, чтобы снизить риск ошибок и предотвратить стандартные атаки, включая переполнение буфера и внесение кода.



9.2.2. Управление внутренней обработкой

Подтверждающие проверки должны быть включены в прикладные программы с целью обнаружения любого искажения информации вследствие ошибок обработки или преднамеренных действий.

Разработка и реализация прикладных программ должны обеспечивать уверенность в том, что риски обработки сбоев, ведущих к потере целостности, сведены к минимуму. Необходимо учитывать, в частности, следующее:

а) использование функций добавления, модификации и удаления для осуществления изменений данных;

б) процедуры, не допускающие запуск программ, исполняемых в неправильной последовательности или исполняемых после сбоя в предшествующей обработке;

в) использование соответствующих программ для восстановления после сбоев и обеспечение правильной обработки данных;

г) защиту от атак, использующих перегрузки/переполнения буфера.

Необходимо подготавливать соответствующую технологическую карту, действия документально оформлять и надежно хранить результаты. Примеры проверок, которые могут быть комбинированными, включают следующее:

а) контроль сеансовой или пакетной обработки с целью согласования остатков массива данных после обновлений в результате транзакции;

б) контроль баланса, чтобы проверить соответствие открываемых данных и данных предыдущего закрытия, а именно:

- меры и средства контроля и управления «от-выполнения-к-выполнению»;
- суммарное количество обновлений файла;
- контроль «от-программы-к-программе»;
- в) подтверждение корректности данных, сгенерированных системой;
- г) проверки целостности, аутентичности или какого-либо другого свойства безопасности, полученных данных или программного обеспечения, или передаваемых между центральным и удаленными компьютерами;
- д) контрольные суммы записей и файлов;
- е) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время;
- ж) проверки для обеспечения уверенности в том, что прикладные программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена;
- з) создание журнала регистрации действий, связанных с обработкой.

Данные, которые были введены правильно, могут быть искажены вследствие аппаратных ошибок, ошибок обработки или преднамеренных действий. Обоснование необходимых проверок зависит от характера прикладной программы и влияния на бизнес любого искажения данных.



9.2.3. Целостность сообщений

Необходимо определить требования в отношении обеспечения аутентичности и защиты целостности сообщений в прикладных программах, а также идентифицировать и внедрить соответствующие меры и средства контроля и управления.

Следует проводить оценку рисков безопасности для определения необходимости обеспечения целостности сообщений, и идентификации соответствующего способа реализации.

Криптографические методы могут использоваться как соответствующее средство реализации аутентификации сообщений.



9.2.4. Подтверждение выходных данных

Данные, выводимые из прикладной программы, должны быть проверены с целью обеспечения уверенности в корректности обработки хранимой информации и соответствия требованиям.

Проверка выходных данных может включать:

- а) проверки достоверности с целью определения приемлемости выходных данных;
- б) контрольная сверка результатов, для обеспечения уверенности в том, что все данные были обработаны;
- в) предоставление достаточной информации для чтения или последующей системы обработки, чтобы определить корректность, полноту, точность и классификацию информации;
- г) процедуры реагирования на проверку пригодности выходных данных;
- д) определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных;
- е) создание журнала регистрации действий по подтверждению корректности выходных данных.

Как правило, системы и прикладные программы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования, выводимые данные будут всегда правильны. Но это не всегда так, т. е. при некоторых обстоятельствах, протестированные системы будут по-прежнему производить некорректные данные вывода.



9.3. Криптографические меры и средства контроля и управления

Цель: Обеспечивать конфиденциальность, аутентичность или целостность информации, используя криптографические средства.

Необходимо разработать политику в отношении использования криптографических мер и средств контроля и управления. Для поддержки использования криптографических методов следует применять управление ключами.

9.3.1. Политика использования криптографических мер и средств контроля и управления

В целях защиты информации необходимо разработать и реализовать политику в отношении использования криптографических мер и средств контроля и управления.

При разработке криптографической политики необходимо учитывать следующее:

а) позицию руководства в отношении использования средств криптографии во всем органе внутренних дел, включая общие принципы, в соответствии с которыми должна быть защищена служебная информация;

б) основанный на оценке риска требуемый уровень защиты, который должен быть определен с учетом типа, стойкости и качества требуемого алгоритма шифрования;

в) использование шифрования для защиты чувствительной информации, передаваемой с помощью переносных или сменных носителей и устройств или по линиям связи;

г) подход к управлению ключами, включая методы по защите криптографических ключей и восстановлению зашифрованной информации в случае потери, компрометации или повреждения ключей;

д) роли и обязанности, например персональная ответственность за:

- внедрение политики;

- управление ключами, включая генерацию ключей;

е) стандарты, которые должны быть приняты для эффективной реализации во всем органе внутренних дел (какое решение используется и для каких процессов служебной деятельности);

ж) влияние использования зашифрованной информации на меры и средства контроля и управления, которые базируются на проверке содержимого (например, обнаружение вирусов).

При внедрении политики безопасности в области криптографии следует учитывать требования законодательства и ограничения, которые могут применяться в отношении криптографических методов в различных странах, а также вопросы трансграничного потока зашифрованной информации.

Криптографические меры и средства контроля и управления могут использоваться для достижения различных целей безопасности, например:

а) конфиденциальности посредством использования шифрования информации для защиты чувствительной или критической информации как хранимой, так и передаваемой;

б) целостности/аутентичности посредством использования электронных подписей или кодов аутентификации сообщений для защиты аутентичности и целостности, хранимой или передаваемой чувствительной или критической информации;

в) неотказуемости, посредством использования криптографических методов для получения подтверждения того, что событие или действие имело или не имело место.

Процесс принятия решения относительно использования криптографии следует рассматривать в рамках более общего процесса оценки рисков и выбора мер и средств контроля и управления. Такая оценка может затем использоваться для определения того, является ли криптографическая мера и средство контроля и управления подходящей, какой тип мер и средств контроля и управления следует применять, с какой целью и для каких процессов служебной деятельности.

Политика использования криптографических мер и средств контроля и управления необходима для того, чтобы максимизировать выгоду и минимизировать риски использования криптографических методов, и чтобы избежать неадекватного или неправильного использования данных средств. При использовании цифровых подписей, необходимо учитывать все применимые требования законодательства, в особенности законодательных актов, описывающих условия, при которых электронная подпись имеет юридическую силу.

9.3.2. Управление ключами

Для поддержки использования органом внутренних дел криптографических методов необходимо применять управление ключами.

Все криптографические ключи следует защищать от модификации, потери и разрушения. Кроме того, секретным и персо-

нальным ключам необходима защита от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей, должно быть физически защищено.

Система управления ключами должна быть основана на согласованном множестве стандартов, процедур и безопасных методов для:

- а) генерации ключей для различных криптографических систем и прикладных программ;
- б) генерации и получения сертификатов открытых ключей;
- в) рассылки ключей предполагаемым пользователям, включая инструкции по активации указанных ключей при получении;
- г) хранения ключей, в том числе инструкций в отношении получения доступа к ключам авторизованных пользователей;
- е) замены или обновления ключей, включая правила в отношении порядка и сроков замены ключей;
- е) действий в отношении скомпрометированных ключей;
- ж) аннулирования ключей, в том числе порядок изъятия и деактивации, например в случае компрометации ключей или при увольнении пользователя из органа внутренних дел (при этом ключи необходимо также архивировать);
- з) восстановления ключей, которые были утеряны или испорчены, как часть управления непрерывностью служебной деятельности, например для восстановления зашифрованной информации;
- и) архивирования ключей, например для восстановления заархивированной или резервной информации;
- к) уничтожения информации;
- л) регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации ключей необходимо, чтобы они имели определенные даты активации и деактивации. Данный период времени зависит от обстоятельств, при которых используются криптографические меры и средства контроля и управления, и от осознаваемого риска.

В дополнение к вопросу безопасности управления криптографическими ключами, необходимо также учитывать вопросы аутентичности открытых ключей. Процесс аутентификации может осуществляться при использовании сертификатов открытых ключей.

чей, которые обычно выдаются органом сертификации, представляющим собой аккредитованный удостоверяющий центр, применяющий соответствующие меры и средства контроля и управления и процедуры для обеспечения требуемой степени доверия.

Необходимо, чтобы соглашение об уровне обслуживания или договоры с внешними поставщиками услуг, связанных с криптографией, например с органом – держателем справочников сертификатов, включали положения относительно ответственности, надежности услуг и времени реагирования на запросы по их предоставлению.

9.4. Безопасность системных файлов

Цель: Обеспечить уверенность в безопасности системных файлов.

Доступ к системным файлам и исходным текстам программ следует контролировать, а проекты ИТ и деятельности по их поддержке необходимо осуществлять безопасным способом. Необходимо проявлять осторожность в среде тестирования, чтобы не подвергать риску чувствительную информацию.

9.4.1. Управление эксплуатируемым программным обеспечением

Необходимо применять процедуры контроля установки программного обеспечения в эксплуатируемых системах.

Для сведения к минимуму риска повреждения эксплуатируемых систем необходимо учесть следующие рекомендации в отношении контроля изменений:

а) обновление эксплуатируемого программного обеспечения, прикладных программ и библиотек программ должны выполнять только обученные администраторы при наличии соответствующего разрешения руководства;

б) эксплуатируемые системы должны содержать только утвержденный исполняемый программный код и не должны содержать коды разработки или компиляторы;

в) прикладные программы и программное обеспечение следует внедрять в эксплуатируемую систему только после всесто-

ронного и успешного тестирования, которое должно выполняться на изолированных системах и включать в себя тесты на пригодность к эксплуатации, безопасность, влияние на другие системы и удобство для пользователя; необходимо обеспечить уверенность в том, что все соответствующие библиотеки исходных текстов программ были обновлены;

г) меры и средства контроля и управления конфигурацией системы необходимо использовать согласно системной документации для сохранения управления всем реализуемым программным обеспечением;

д) прежде чем изменения будут реализованы, необходимо применять метод отката;

е) в контрольном журнале должны быть сохранены все обновления эксплуатируемой библиотеки программ;

ж) предыдущие версии прикладного программного обеспечения следует сохранять на случай непредвиденных обстоятельств;

з) старые версии программного обеспечения следует архивировать вместе со всей требуемой информацией и параметрами, процедурами, конфигурационными деталями и поддерживающим программным обеспечением до тех пор, пока данные хранятся в архиве.

Необходимо, чтобы поставляемое поставщиком программное обеспечение, используемое в действующей системе, поддерживалось на уровне, обеспечиваемом поставщиком. Со временем поставщики программного обеспечения прекращают поддерживать более старые версии программного обеспечения. Орган внутренних дел должен учитывать риски, когда он полагается на неподдерживаемое программное обеспечение.

Любое решение об обновлении программного обеспечения до новой версии должно учитывать требования служебной деятельности в отношении изменения и безопасности новой версии, т. е., введение новых функциональных возможностей безопасности или количество и серьезность проблем безопасности, связанных с этой версией. Исправления (патчи) программного обеспечения следует применять, если они помогают удалять или снижать уязвимости безопасности.

Физический или логический доступ следует предоставлять поставщикам только для целей поддержки, по мере необходимо-

сти и на основании разрешения руководства. Действия поставщика должны подвергаться мониторингу.

Программное обеспечение компьютеров может использовать поставляемые внешним (иностранным) поставщиком программное обеспечение и модули, которые должны быть контролируемы и управляемы во избежание несанкционированных изменений, которые могут способствовать нарушению безопасности.

Эксплуатируемую систему следует обновлять только при необходимости, например, если текущая версия эксплуатируемой системы больше не удовлетворяет требованиям служебной деятельности. Обновление не следует проводить только потому, что доступна новая версия для эксплуатируемой системы. Новые версии систем, находящихся в промышленной эксплуатации, могут быть менее безопасными, менее стойкими и менее понятными, чем текущие системы.



9.4.2. Защита тестовых данных системы

Данные тестирования следует тщательно отбирать, защищать и контролировать.

Следует избегать использования действующих баз данных, содержащих персональную или какую-либо другую чувствительную информацию, для целей тестирования. Если персональная или какая-либо другая чувствительная информация требуется для тестирования, то все чувствительные подробности и информационное наполнение следует удалить или изменить до неузнаваемости перед использованием. Для защиты действующих (рабочих) данных, если они используются для целей тестирования, необходимо применять следующие рекомендации:

а) процедуры управления доступом, применимые для эксплуатируемых прикладных систем, следует также применять и для тестирования прикладных систем;

б) необходимо отдельное разрешение на каждый случай копирования действующей (рабочей) информации для тестирования прикладной системы;

в) после того, как тестирование было завершено, действующую (рабочую) информацию следует немедленно удалить из тестируемой прикладной системы;

г) копирование и использование действующей (рабочей) информации должно фиксироваться для обеспечения контрольной записи.

Для осуществления системного или приемочного тестирования обычно требуется существенный объем тестовых данных, которые максимально приближены к действующим (рабочим) данным.



9.4.3. Управление доступом к исходным текстам программ

Доступ к исходным текстам программ необходимо ограничивать.

В целях предотвращения введения несанкционированных функциональных возможностей и во избежание непреднамеренных изменений должен быть обеспечен строгий контроль доступа к исходным текстам программ и связанным с ними документам (например проектам, спецификациям, планам верификации и планам валидации). В отношении исходных текстов программ это может быть достигнуто с помощью контролируемого централизованного хранения таких текстов, предпочтительнее в библиотеках исходных текстов программ. Чтобы сократить возможность искажения компьютерных программ, необходимо рассмотреть следующие рекомендации по управлению доступом к таким библиотекам исходных текстов программ:

а) по возможности, следует избегать хранения библиотек исходных текстов программ в эксплуатируемых системах;

б) управление исходных текстов программ и библиотек исходных текстов программ следует осуществлять в соответствии с установленными процедурами;

в) персонал поддержки не должен иметь неограниченный доступ к библиотекам исходных текстов программ;

г) обновление библиотек исходных текстов программ и связанных с ними элементов, а также предоставление программистам исходных текстов программ должны осуществляться только после получения соответствующего разрешения;

д) распечатки (листинги) программ следует хранить безопасным образом;

е) в контрольном журнале должны фиксироваться все обращения к библиотекам исходных текстов программ;

ж) поддержку и копирование библиотек исходных текстов программ следует осуществлять в соответствии со строгими процедурами контроля изменений.

Исходный текст программы – это текст, написанный программистами, который компилируется (и компоуется) с целью создания исполняемых файлов. Определенные языки программирования формально не проводят различия между исходным текстом программ и исполняемыми файлами, поскольку исполняемые файлы создаются в то время, когда они активированы.



В ГОСТ Р ИСО 10007-2007 [21] содержится дополнительная информация об управлении конфигурацией и о процессе, связанном с жизненным циклом программного обеспечения.

9.5. Безопасность в процессах разработки и поддержки

Цель: Поддерживать безопасность прикладных систем и информации.

Необходимо строго контролировать среды проектирования и поддержки.

Необходимо, чтобы руководители, ответственные за прикладные системы, также несли ответственность и за безопасность среды проектирования или поддержки. Они должны обеспечить уверенность в том, что все предложенные изменения системы проанализированы на предмет возможных нарушений безопасности системы или условий эксплуатации.

9.5.1. Процедуры управления изменениями

Внесение изменений следует контролировать, используя формальные процедуры управления изменениями.

Для сведения к минимуму повреждений информационных систем следует осуществлять и документально оформлять фор-

мальные процедуры контроля изменений. Введение новых и значительные изменения существующих систем должны сопровождаться формальным процессом документального оформления, детализирования, тестирования, контроля качества и управляемого внедрения.

Указанный процесс должен включать в себя оценку рисков, анализ влияния изменений и детализацию необходимых мер и средств контроля и управления безопасностью. Он также должен обеспечивать уверенность в том, что не нарушены безопасность и сами процедуры управления, что программистам, отвечающим за поддержку, предоставлен доступ только к тем частям системы, которые необходимы для их работы, и что любые изменения формально согласованы и одобрены.

По возможности, прикладные программы и эксплуатационные процедуры управления изменениями должны быть интегрированы. Процедуры изменения должны включить:

- а) ведение учета согласованных уровней разрешений;
- б) обеспечение уверенности в том, что изменения представлены уполномоченными пользователями;
- в) анализ мер и средств контроля и управления, а также процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями;
- г) выявление всего программного обеспечения, информации, объектов баз данных и аппаратных средств, требующих изменений;
- д) получение формального одобрения на детальные предложения по изменениям перед началом работы;
- е) обеспечение уверенности в том, что авторизованный пользователь одобрил все изменения до их реализации;
- ж) обеспечение уверенности в том, что комплект системной документации обновляется после завершения каждого изменения, и что старая документация архивируется или удаляется;
- з) поддержание управления версиями для всех обновлений программного обеспечения;
- и) сохранение контрольных записей обо всех запросах на изменение;

к) обеспечение уверенности в том, что эксплуатационная документация и пользовательские процедуры при необходимости изменяются, чтобы соответствовать внесенным изменениям;

л) обеспечение уверенности в том, что процесс внедрения изменений осуществляется в согласованное время и не нарушает затрагиваемых процессов служебной деятельности.

Изменение в программном обеспечении может повлиять на среду эксплуатации.

Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, которая отделена от среды эксплуатации и среды разработки. Это обеспечивает средства контроля над новым программным обеспечением, и предоставляет дополнительную защиту действующей (рабочей) информации, используемой в целях тестирования. Для этих целей следует использовать изменения (патчи), служебные пакеты обновлений и другие обновления. Автоматические обновления не следует применять в критических системах, поскольку некоторые обновления могут являться причиной отказа критических прикладных программ.



9.5.2. Техническая проверка прикладных программ после изменений эксплуатируемой системы

При внесении изменений в эксплуатируемые системы прикладные программы, имеющие большое значение для служебной деятельности, следует анализировать и тестировать с целью обеспечения уверенности в том, что не оказывается неблагоприятного воздействия на функционирование или безопасность органа внутренних дел.

Этот процесс должен охватывать:

а) анализ мер и средств контроля и управления прикладными программами и процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями эксплуатируемой системы;

б) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, необходимые при изменениях эксплуатируемой системы;

в) обеспечение уверенности в том, что уведомления об изменениях эксплуатируемой системы поступают своевременно, чтобы дать возможность перед их реализацией провести соответствующие тесты и анализы;

г) обеспечение уверенности в том, что соответствующие изменения вносятся в планы обеспечения непрерывности служебной деятельности.

Определенной группе лиц или отдельному специалисту следует вменить в обязанность проведение мониторинга уязвимостей, версий патчей поставщиков и их установок.

9.5.3. Ограничения на изменения пакетов программ

Необходимо избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все сделанные изменения.

Насколько возможно и допустимо с практической точки зрения пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

а) риск в отношении встроенных мер и средств контроля и управления и процедур обеспечения целостности;

б) необходимость получения согласия поставщика;

в) возможность получения требуемых изменений от поставщика в качестве стандартной программы обновления;

г) возможные последствия в случае, если орган внутренних дел станет ответственным за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ. Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

9.5.4. Утечка информации

Возможность утечки информации должна быть предотвращена.

Для снижения риска утечки информации, например по причине использования и эксплуатации скрытых каналов, необходимо принимать во внимание следующее:

а) сканирование носителей исходящей информации и каналов связи на наличие скрытой информации;

б) маскирование и регулирование поведения систем и каналов связи для снижения вероятности того, что третья сторона сможет извлечь информацию из поведения систем и каналов связи;

в) использование систем и программного обеспечения, которые считаются максимально достоверными, например использование оцененных продуктов (см. ГОСТ Р ИСО/МЭК 15408-1-2012 [22]);

г) регулярный мониторинг деятельности персонала и систем там, где это разрешено существующим законодательством или предписаниями;

д) мониторинг использования ресурсов в компьютерных системах.

Скрытые каналы – это каналы, не предназначенные для передачи информационных потоков, но которые, тем не менее, могут существовать в системе или сети. Например, манипулирование битами в пакетах протоколов связи может использоваться как скрытый метод передачи сигналов. Природа скрытых каналов такова, что предотвратить существование всех возможных скрытых каналов затруднительно или даже невозможно. Однако такие каналы часто используются «троянскими» программами. Следовательно, принятие мер по защите от «троянских» программ снижает риск использования скрытых каналов.



Предотвращение неавторизованного доступа к сети, а также политики и процедуры, препятствующие неправильному использованию информационных услуг персоналом, способствуют защите от скрытых каналов.

9.5.5. Аутсорсинг разработки программного обеспечения

Аутсорсинг разработки программного обеспечения должен быть под наблюдением и контролем органа внутренних дел.

Там, где для разработки программного обеспечения привлекается сторонняя организация, необходимо учитывать следующее:

- а) лицензионные соглашения, права собственности на программы и права интеллектуальной собственности;
- б) сертификацию качества и точности выполненной работы;
- в) соглашения условного депонирования на случай отказа сторонней организации выполнять свои обязательства;
- г) права доступа с целью проверки качества и точности сделанной работы;
- д) договорные требования к качеству и функциональной безопасности программ;
- е) тестирование программ перед установкой на предмет обнаружения вредоносных и «тройанских» программ.

9.6. Управление техническими уязвимостями

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей.

Управление техническими уязвимостями следует осуществлять эффективным, систематическим и повторяемым способом, с проведением измерений с целью подтверждения его эффективности. Эти соображения должны касаться эксплуатируемых систем и любых других используемых прикладных программ.

Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать незащищенность органа внутренних дел в отношении таких уязвимостей и принимать соответствующие меры для рассмотрения связанного с ними риска.

Постоянно обновляемая и полная опись активов является предпосылкой эффективного управления техническими уязвимостями. Специальная информация, необходимая для поддержки управления техническими уязвимостями, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии развертывания (например какое про-

граммное обеспечение установлено на каких системах) и специалисте(ах), отвечающем(их) в органе внутренних дел за программное обеспечение.

Аналогично, своевременное действие должно предприниматься в ответ на выявление потенциальных технических уязвимостей. Для создания эффективного процесса управления в отношении технических уязвимостей необходимо выполнять следующие рекомендации:

а) в органе внутренних дел необходимо определять и устанавливать роли и обязанности, связанные с управлением техническими уязвимостями, включая мониторинг уязвимостей, оценку риска проявления уязвимостей, исправление программ (патчинг), слежение за активами и любые другие координирующие функции;

б) информационные ресурсы, которые будут использоваться для выявления значимых технических уязвимостей и обеспечения осведомленности о них, следует определять для программного обеспечения и другой технологии на основе списка инвентаризации активов; эти информационные ресурсы должны обновляться вслед за изменениями, вносимыми в опись, или когда найдены другие новые или полезные ресурсы;

в) необходимо определить временные параметры реагирования на уведомления о потенциально значимых технических уязвимостях;

г) после выявления потенциальной технической уязвимости орган внутренних дел должен определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать внесение исправлений в уязвимые системы и (или) применение других мер и средств контроля и управления;

д) в зависимости от того, насколько срочно необходимо рассмотреть техническую уязвимость, предпринимаемое действие следует осуществлять в соответствии с мерами и средствами контроля и управления, связанными с управлением изменений, или следуя процедурам реагирования на инциденты информационной безопасности;

е) если имеется возможность установки патча, следует оценить риски, связанные с его установкой (риски, создаваемые уязвимостью, необходимо сравнить с риском установки патча);

ж) перед установкой патчи следует тестировать и оценивать для обеспечения уверенности в том, что они являются эффективными и не приводят к побочным эффектам, которые нельзя допускать; если нет возможности установить патч, следует рассмотреть другие меры и средства контроля и управления, например:

- отключение сервисов, связанных с уязвимостью;
- адаптацию или добавление средств управления доступом, например межсетевых экранов на сетевых границах;
- усиленный мониторинг для обнаружения или предотвращения реальных атак;
- повышение осведомленности об уязвимостях;

з) в контрольный журнал следует вносить информацию о всех предпринятых процедурах;

и) следует регулярно проводить мониторинг и оценку процесса управления техническими уязвимостями в целях обеспечения уверенности в его эффективности и действенности;

к) в первую очередь следует обращать внимание на системы с высоким уровнем риска.

Правильное функционирование процесса управления техническими уязвимостями играет важную роль для многих органов внутренних дел, поэтому процесс должен подвергаться регулярному мониторингу. Для обеспечения уверенности в том, что потенциально значимые технические уязвимости выявлены, важна точная инвентаризация.

Управление техническими уязвимостями может рассматриваться как подфункция управления изменениями и в качестве таковой может воспользоваться процессами и процедурами управления изменениями.

Поставщики часто испытывают на себе значительное давление, заключающееся в требовании выпускать патчи в кратчайшие сроки. Поэтому патч не может решить проблему адекватно и может иметь побочные эффекты. К тому же, в некоторых случаях, если патч был однажды применен, деинсталлировать его может быть нелегко.

Если адекватное тестирование патчей провести не удастся, например по причине затрат или отсутствия ресурсов, можно рассмотреть задержку в осуществлении внесения изменений, чтобы оценить связанные с этим риски, основанные на опыте других пользователей.



10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Оповещение о событиях и уязвимостях информационной безопасности

Цель: Обеспечить уверенность в том, что о событиях и уязвимостях информационной безопасности оповещение осуществляется способом, который позволяет своевременно предпринять корректирующее действие.

Необходимо использовать формальные процедуры информирования и эскалации. Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о процедурах информирования, о различных типах событий и уязвимостях, которые могли бы оказать негативное влияние на безопасность активов органа внутренних дел. Они должны незамедлительно сообщать о любых событиях и уязвимостях информационной безопасности определенному контактному лицу.

В контексте управления инцидентами информационной безопасности под термином «процедуры эскалации» понимается передача расследования инцидента на более высокий уровень в случае невозможности проведения адекватного расследования на более низком уровне.

10.1.1. Оповещение о событиях информационной безопасности

О событиях информационной безопасности необходимо незамедлительно сообщать через соответствующие каналы управления.

Необходимо внедрить формальную процедуру оповещения о событиях информационной безопасности вместе с процедурой реагирования и эскалации инцидента, содержащую действие, которое нужно предпринять при получении сообщения о событии информационной безопасности. Должна быть установлена «точка контакта» для уведомления о событиях информационной безопасности. Необходимо обеспечить уверенность в том, что эта «точка

контакта» известна в органе внутренних дел, всегда доступна и способна к адекватному и своевременному реагированию.

Все сотрудники, подрядчики и представители третьей стороны должны быть осведомлены о своей обязанности незамедлительно сообщать о любых событиях информационной безопасности. Они должны быть также осведомлены о процедуре информирования о событиях информационной безопасности и «точке контакта». Необходимо, чтобы процедуры информирования включали:

а) соответствующие процессы обратной связи, для обеспечения уверенности в том, что сотрудник, сообщивший о событиях информационной безопасности, был уведомлен о результатах после того, как проблема была решена и закрыта;

б) формы сообщений о событиях информационной безопасности, которые должны напомнить лицу о действиях, которые необходимо совершить;

в) правила поведения в случае, если произойдет событие информационной безопасности, а именно:

- сразу же обращать внимание на все важные детали (например, тип несоответствия или недостатка, возникшие неисправности, сообщения на экране, странное поведение);

- не предпринимать самостоятельно никакого действия, а немедленно сообщить в «точку контакта»;

- ссылку на установленные формальные дисциплинарные процессы относительно сотрудников, подрядчиков и пользователей третьей стороны, которые нарушают правила безопасности.

Среда с высоким уровнем риска может быть оснащена сигнализацией о принуждении, с помощью которой лица, на которые оказывается давление, могут указать на такие проблемы. Процедура реагирования на сигнализацию о принуждении должна отражать место высокого риска, которое показывает сигнализация.

Сигнализация о принуждении – это способ, с помощью которого можно незаметно показать, что действие совершается «под принуждением».

Примерами событий и инцидентов информационной безопасности могут быть:

- а) потеря услуг, оборудования или средств обслуживания;
- б) неисправности в системе или перегрузки;
- в) ошибки оператора;
- г) несоблюдение политик или рекомендаций;
- д) нарушения мер физической безопасности;
- е) неконтролируемые изменения систем;
- ж) программный или аппаратный сбой;
- з) нарушения доступа.

Обращая должное внимание на аспекты конфиденциальности, можно для повышения осведомленности пользователей использовать инциденты информационной безопасности в качестве примеров того, что могло бы произойти, как реагировать на такие инциденты и как избежать их в будущем. Чтобы иметь возможность должным образом рассмотреть события и инциденты информационной безопасности, необходимо собирать свидетельства как можно быстрее после происшествия.

Неисправная работа или другое аномальное поведение системы может служить показателем атаки на безопасность или реального недостатка безопасности, поэтому о них следует сообщать как о событии информационной безопасности.

Дополнительную информацию относительно отчетности о событиях информационной безопасности и об управлении инцидентами информационной безопасности можно найти в ГОСТ Р ИСО/МЭК ТО 18044-2007 [23].



10.1.2. Оповещение об уязвимостях безопасности

От всех сотрудников, подрядчиков и представителей третьей стороны, имеющих дело с информационными системами и услугами, необходимо требовать, чтобы они обращали внимание и сообщали о любых замеченных или предполагаемых уязвимостях в области безопасности в отношении систем или услуг.

Все сотрудники, подрядчики и представители третьей стороны должны как можно быстрее сообщать об уязвимостях безопасности своему руководству или непосредственно поставщику услуг, чтобы предотвратить инциденты информационной безопасности. Механизм сообщения должен быть, насколько возможно, простым и доступным. Сотрудников, подрядчиков и представителей третьей стороны необходимо проинформировать о недопустимости попыток проверить предполагаемый недостаток.

Сотрудникам, подрядчикам и представителям третьей стороны рекомендуется не проверять предполагаемые недостатки безопасности. Тестирование слабых мест защиты может быть интерпретировано как неправомерное использование системы, а также может нанести ущерб информационной системе или услуге и привести к юридической ответственности лица, выполнившего тестирование.



10.2. Управление инцидентами информационной безопасности и необходимое совершенствование

Цель: Обеспечить уверенность в том, что в отношении управления инцидентами информационной безопасности применяется последовательный и эффективный подход.

Обязанности и процедуры должны осуществляться эффективным способом в отношении обработки событий и уязвимостей информационной безопасности, как только они были зарегистрированы. Процесс постоянного совершенствования необходимо применять в отношении мониторинга, оценки, общего управления и реагирования на инциденты информационной безопасности.

Необходимо собирать доказательства, чтобы обеспечить уверенность в соответствии законодательным требованиям.

10.2.1. Обязанности и процедуры

Необходимо устанавливать обязанности должностных лиц по осуществлению управления и процедуры для обеспечения быстрого, эффективного и должного реагирования на инциденты информационной безопасности.

В дополнение к информированию о событиях и недостатках информационной безопасности, необходимо также использовать мониторинг систем, сигналов тревоги и уязвимостей для обнаружения инцидентов информационной безопасности. В отношении процедур управления инцидентами информационной безопасности необходимо учитывать следующие рекомендации:

а) следует установить процедуры обработки различных типов инцидентов информационной безопасности, включая:

- сбои информационных систем и потерю обслуживания;
- вредоносные программы;
- отказ в обслуживании;
- ошибки, являющиеся следствием неполноты или неточности данных служебной деятельности;
- нарушения конфиденциальности и целостности;
- неправильное использование информационных систем;

б) в дополнение к обычным планам обеспечения непрерывности служебной деятельности, процедуры должны также охватывать:

- анализ и выявление причины инцидента;
- ограничение распространения последствий;
- планирование и реализацию корректирующего действия для предотвращения повторения, если это необходимо;
- взаимодействие с лицами, испытывавшими влияние инцидента или участвовавшими в восстановлении после инцидента;
- сообщение о предпринятом действии в соответствующий орган;

в) контрольные записи и аналогичные доказательства необходимо собирать и защищать для:

- анализа внутренних проблем;
- использования в качестве судебного доказательства в отношении возможного нарушения договора или нормативного

требования, а также в случае гражданского или уголовного производства, например на основании неправильного использования компьютера или законодательства о защите данных;

- обсуждения условий о выплате компенсации поставщиками программного обеспечения и услуг;

г) действия по восстановлению после проявления недостатков безопасности и по устранению сбоев систем следует тщательно контролировать; процедуры должны обеспечивать уверенность в том, что:

- только четко идентифицированному и уполномоченному персоналу разрешен доступ к эксплуатируемым системам и данным;

- все предпринятые аварийные действия документируются в деталях;

- руководство информируется об аварийном действии, и такое действие анализируется должным образом;

- целостность систем, а также мер и средств контроля и управления служебной деятельности подтверждается с минимальной задержкой.

Цели управления инцидентами информационной безопасности следует согласовать с руководством, а также необходимо обеспечить уверенность в том, что лица, ответственные за осуществление управления инцидентами информационной безопасности, понимают приоритеты органа внутренних дел по обработке таких инцидентов.

Инциденты информационной безопасности могут выходить за границы органа внутренних дел и стран. В отношении реагирования на такие инциденты имеется растущая потребность в координации реагирования и в совместном использовании информации об этих инцидентах с внешними организациями при необходимости.



10.2.2. Извлечение уроков из инцидентов информационной безопасности

Должны быть созданы механизмы, позволяющие установить типы, объемы и убытки, вызванные инцидентами информационной безопасности, которые должны быть измерены и проконтролированы.

Информацию, полученную в результате оценки инцидентов информационной безопасности, следует использовать для идентификации повторяющихся или оказывающих значительное влияние инцидентов.

Оценка инцидентов информационной безопасности может указывать на необходимость совершенствования существующих мер или внедрения дополнительных мер и средств контроля и управления, чтобы снизить частоту, ущерб и стоимость возможных происшествий, или должна быть принята во внимание при пересмотре политики безопасности.



10.2.3. Сбор доказательств

В тех случаях, когда последующие действия против лица или органа внутренних дел после инцидента безопасности приводят к судебному иску (как гражданскому, так и уголовному), доказательства должны быть собраны, сохранены и представлены в соответствии с правилами сбора доказательств.

При сборе и представлении доказательства для целей дисциплинарных воздействий, рассматриваемых в рамках органа внутренних дел, необходимо разработать и обеспечить следование внутренним процедурам.

В основном, правила, применяемые в отношении сбора доказательств, предусматривают:

- а) допустимость доказательств, т. е. может ли доказательство использоваться в суде;
- б) весомость доказательств, т. е. качество и полнота доказательств.

Чтобы добиться признания допустимости доказательств, органу внутренних дел необходимо быть уверенными в том, что их информационные системы соответствуют любому изданному стандарту или своду правил в отношении предъявления допустимых доказательств.

Весомость предъявляемых доказательств должна соответствовать любым применимым требованиям. Чтобы добиться признания весомости доказательств, необходимы убедительные подтверждения того, что для корректной и последовательной защиты доказательств в течение периода их хранения и обработки применялись меры и средства контроля и управления соответствующего качества и полноты (т. е. доказательство управляемости процесса). В общем случае такие убедительные подтверждения могут быть получены следующим образом:

а) для бумажных документов: оригинал должен храниться безопасным способом, и должно быть зафиксировано лицо, нашедшее документ, место и время нахождения документа и свидетели находки; любое исследование должно удостоверить, что оригиналы не подделаны;

б) для информации на компьютерных носителях: зеркальное отображение или копии (в зависимости от применимых требований) любых сменных носителей, информации на жестких дисках или основной памяти компьютера следует выполнять таким образом, чтобы обеспечить доступность; журнал регистрации всех действий в течение процесса копирования необходимо сохранить, а сам процесс копирования удостоверить; оригиналы носителей информации и журнал регистрации (если это не представляется возможным, то, по крайней мере, один зеркальный образ или копию) следует хранить надежно и без изменений.

Любое судебное разбирательство должно проводиться только по копиям доказательного материала. Целостность доказательного материала необходимо защищать. Копирование доказательного материала должно контролироваться заслуживающим доверия персоналом, а информация о том, когда и где осуществлялся процесс копирования, кто этим занимался, и какие инструментальные средства и программы были использованы, должна регистрироваться.

Когда событие информационной безопасности обнаруживаются впервые, не очевидно, приведет ли оно к судебным разбирательствам или нет. Поэтому существует опасность того, что необходимое доказательство будет уничтожено преднамеренно или случайно прежде, чем будет осознана серьезность инцидента. Целесообразно на самом раннем этапе привлечь юриста или специалиста в любом случае предполагаемых судебных разбирательств, и получить консультацию относительно требуемых доказательств.

Доказательство может выходить за границы орган внутренних дел и (или) юрисдикции. В таких случаях, следует обеспечивать уверенность в том, что орган внутренних дел имеет право сбора необходимой информации в качестве доказательства. Необходимо также учитывать требования различных юрисдикций, чтобы максимально увеличить шанс признания доказательства в рамках соответствующих юрисдикций.



11. УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ ДЕЯТЕЛЬНОСТИ

11.1. Аспекты информационной безопасности в рамках управления непрерывностью служебной деятельности

Цель: Противодействовать прерываниям видов деятельности в рамках служебной деятельности органа внутренних дел и защищать важнейшие процессы служебной деятельности от последствий значительных сбоев информационных систем или чрезвычайных ситуаций и обеспечивать их своевременное возобновление.

Необходимо внедрить процесс управления непрерывностью служебной деятельности с целью минимизации негативного влияния на орган внутренних дел и восстановления после потери информационных активов (которые могут быть результатом, например стихийных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мер и средств контроля и управления. Указанный процесс должен выявлять критические процессы служебной деятельности и объединять требования к управлению информационной безопасности в части непрерывности служебной деятельности с другими требованиями по обеспечению непрерывности, касающимися функционирования оборудования.

Последствия стихийных бедствий, нарушений безопасности, отказов в обслуживании и потери доступности обслуживания необходимо анализировать на предмет их влияния на служебную деятельность. Необходимо разработать и внедрить планы обеспечения непрерывности служебной деятельности с целью обеспечения уверенности в том, что значимые операции могут быть возобновлены в течение требуемого времени. Информационная безопасность должна стать составной частью всего процесса обеспечения непрерывности служебной деятельности и других процессов управления, реализуемых в органе внутренних дел.

Необходимо, чтобы управление непрерывности служебной деятельности включало в себя меры и средства контроля и управления по выявлению и снижению рисков в дополнение к общему

процессу оценки рисков, ограничения последствий разрушительных инцидентов и обеспечения уверенности в том, что информация, требуемая для процессов служебной деятельности, легко доступна.

11.1.1. Включение информационной безопасности в процесс управления непрерывностью служебной деятельности

Следует разрабатывать и поддерживать управляемый процесс для обеспечения непрерывности служебной деятельности во всем органе внутренних дел, который учитывает требования к информационной безопасности, необходимые для обеспечения непрерывности служебной деятельности органа внутренних дел.

Данный процесс должен объединять следующие ключевые элементы управления непрерывностью служебной деятельности:

а) понимание рисков, с которыми сталкивается орган внутренних дел, с точки зрения вероятности и продолжительности воздействия, включая определение критических процессов служебной деятельности и установление их приоритетов;

б) определение всех активов, вовлеченных в критические процессы служебной деятельности;

в) понимание последствий для служебной деятельности, которые могут быть вызваны прерываниями, обусловленными инцидентами информационной безопасности (важно, чтобы были найдены решения, которые будут применяться как в случае незначительных, так и существенных инцидентов, потенциально угрожающих жизнедеятельности органа внутренних дел), а также определение целей служебной деятельности применительно к средствам обработки информации;

г) определение и рассмотрение возможности внедрения дополнительных превентивных и нейтрализующих мер и средств контроля и управления;

д) определение достаточности финансовых, организационных, технических ресурсов и ресурсов окружающей среды для реагирования на выявленные требования информационной безопасности;

е) обеспечение безопасности персонала и защита средств обработки информации и имущества органа внутренних дел;

ж) разработку и документальное оформление планов обеспечения непрерывности служебной деятельности, учитывающих требования информационной безопасности в соответствии с согласованной стратегией обеспечения непрерывности служебной деятельности;

з) регулярное тестирование и обновление данных планов и применяемых процессов;

и) обеспечение уверенности в том, что управление непрерывностью служебной деятельности органично вписывается в процессы и структуру органа внутренних дел; ответственность за процесс управления информационной безопасностью следует назначать на соответствующем уровне в рамках органа внутренних дел.

11.1.2. Непрерывность служебной деятельности и оценка риска

События, которые могут стать причиной прерываний процессов служебной деятельности, необходимо определять вместе с вероятностью и влиянием таких прерываний, а также их последствиями для информационной безопасности.

Необходимо, чтобы аспекты информационной безопасности в контексте обеспечения непрерывности служебной деятельности основывались на выявлении событий (или последовательности событий), которые могут стать причиной прерываний служебных процессов органа внутренних дел, например отказ оборудования, ошибки оператора, кража, пожар, стихийные бедствия и терроризм. Данный процесс должен сопровождаться оценкой рисков с целью определения вероятности и последствий указанных прерываний с точки зрения времени, масштаба повреждения и периода восстановления.

Оценки рисков в отношении непрерывности служебной деятельности необходимо осуществлять при непосредственном участии владельцев ресурсов используемых в служебной деятельности и процессах. Данная оценка должна охватывать все процессы служебной деятельности и не ограничиваться средствами обработки информации, но она должна учитывать результаты, отно-

сящиеся к информационной безопасности. Важно объединить различные аспекты риска, чтобы получить полную картину требований органа внутренних дел в отношении непрерывности служебной деятельности. Оценка должна идентифицировать риски, определять их количество и приоритет по отношению к критериям и целям, имеющим значение для органа внутренних дел, включая критические ресурсы, последствия нарушений, допустимое время простоя и приоритеты восстановления.

В зависимости от результатов оценки рисков, необходимо разработать стратегию, чтобы определить общий подход к обеспечению непрерывности служебной деятельности. После того как эта стратегия будет разработана, необходимо, чтобы она была утверждена руководством, а также, чтобы был разработан и утвержден план реализации данной стратегии.

11.1.3. Разработка и внедрение планов обеспечения непрерывности служебной деятельности, учитывающих информационную безопасность

Следует разработать и внедрить планы обеспечения непрерывности служебной деятельности с целью поддержки или восстановления операций и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или сбоя критических процессов служебной деятельности.

Процесс планирования непрерывности служебной деятельности должен предусматривать следующее:

- а) определение и согласование всех обязанностей и процедур, связанных с обеспечением непрерывности служебной деятельности;
- б) определение приемлемых потерь информации и услуг;
- в) внедрение процедур, позволяющих восстановить и возобновить операции служебной деятельности и доступность информации в требуемые сроки; особое внимание следует уделить оценке внешних и внутренних зависимостей служебной деятельности и существующих договоров;
- г) эксплуатационные процедуры, которым необходимо следовать в ожидании завершения восстановления и возобновления;

д) документальное оформление согласованных процедур и процессов;

е) соответствующее обучение сотрудников согласованным процедурам и процессам, включая управление в критических ситуациях;

ж) тестирование и обновление планов.

Необходимо, чтобы в процессе планирования особое внимание было обращено на требуемые цели служебной деятельности, например восстановление определенных услуг связи для клиентов в приемлемые сроки. Следует учитывать потребность в необходимых для этого услугах и ресурсах, включая укомплектованность персоналом, ресурсы, не связанные с обработкой информации, а также меры по переходу на аварийный режим средств обработки информации. Такие меры по переходу на аварийный режим могут включать в себя договоренности с третьей стороной в виде взаимных соглашений или коммерческих абонируемых услуг.

Планы обеспечения непрерывности служебной деятельности должны учитывать уязвимости органа внутренних дел и поэтому могут содержать чувствительную информацию, нуждающуюся в соответствующей защите. Копии планов обеспечения непрерывности служебной деятельности следует хранить на достаточном расстоянии от основного здания, чтобы избежать их повреждения вследствие аварии в основном здании. Руководство должно обеспечить уверенность в том, что обновление и защита планов обеспечения непрерывности служебной деятельности осуществляется на том же уровне, что и в основном здании. Другие материалы, необходимые для выполнения планов по обеспечению непрерывности служебной деятельности, следует также хранить в удаленном месте.

Если для хранения используются различные временные помещения, то уровень реализуемых мер и средств контроля и управления безопасности в таких помещениях должен соответствовать уровню мер, реализуемых в основном здании.

Следует заметить, что планы по управлению в критических ситуациях и действия могут отличаться от управления непрерывностью служебной деятельности, т. е. кризис может быть улажен обычными процедурами управления.



11.1.4. Основы планирования непрерывности служебной деятельности

Следует поддерживать единую структуру планов непрерывности служебной деятельности, чтобы обеспечить уверенность в том, что все планы согласованы в соответствии с рассматриваемыми требованиями информационной безопасности и установленными приоритетами для тестирования и обслуживания.

В каждом плане обеспечения непрерывности служебной деятельности должен описываться подход к обеспечению непрерывности, например подход к обеспечению уверенности в доступности и безопасности информации или информационных систем. Каждый план должен определять план эскалации (расширения) и условия активизации, а также лиц, ответственных за выполнение каждого пункта плана. При появлении новых требований любые существующие процедуры на случай чрезвычайных ситуаций, например планы эвакуации или меры по переходу на аварийный режим, при необходимости следует корректировать. Процедуры должны быть включены в программу управления изменений орган внутренних дел с целью обеспечения уверенности в том, что вопросы обеспечения непрерывности служебной деятельности рассматриваются всегда соответствующим образом.

Каждый план должен иметь определенного владельца. Процедуры на случай чрезвычайных ситуаций, планы по переходу на аварийный режим, планы по возобновлению следует включать в сферу ответственности владельцев соответствующих ресурсов, используемых в служебной деятельности или вовлеченных процессов. Ответственность за меры по переходу на аварийный режим альтернативных технических услуг, таких как обработка информации и средства связи, обычно несут поставщики услуг.

В основу планирования непрерывности служебной деятельности должны быть заложены требования информационной безопасности, и предусмотрено следующее:

а) условия активизации планов, описывающие процесс, которому необходимо следовать (например, как оценить ситуацию, кто должен принимать участие), прежде чем привести в действие каждый план;

б) процедуры, определяющие порядок действий при чрезвычайных ситуациях, которые должны быть предприняты после инцидента, ставящего под угрозу операции служебной деятельности;

в) процедуры перехода на аварийный режим, описывающие действия, которые должны быть предприняты, чтобы перенести важные операции служебной деятельности и услуги поддержки в альтернативное временное место размещения и восстановить процессы служебной деятельности в требуемые сроки;

г) временные эксплуатационные процедуры, которых следует придерживаться в ожидании завершения восстановления и возобновления;

д) процедуры возобновления, определяющие порядок действий, которые должны быть предприняты, чтобы вернуться к нормальному состоянию операций служебной деятельности;

е) график поддержки плана, который определяет способ и время проверки, а также процесс поддержки плана в актуальном состоянии;

ж) информирование, обучение и тренинг, направленные на понимание процессов обеспечения непрерывности служебной деятельности и обеспечение уверенности в эффективности этих процессов;

з) обязанности лиц с указанием ответственных за выполнение каждого пункта плана, при необходимости должны быть указаны альтернативные ответственные лица;

и) важнейшие активы и ресурсы, необходимые для действий в чрезвычайных ситуациях, при переходе на аварийный режим и в процедурах возобновления.

11.1.5. Тестирование, поддержка и пересмотр планов непрерывности служебной деятельности

Планы непрерывности служебной деятельности необходимо регулярно тестировать и обновлять с целью обеспечения уверенности в их актуальности и эффективности.

Указанные тесты должны обеспечивать уверенность в том, что все члены группы ликвидации последствий чрезвычайных ситуаций и другой персонал, имеющий к этому отношение, осве-

домлены о планах и о своих обязанностях, касающихся обеспечения непрерывности служебной деятельности и информационной безопасности.

В графике тестирования плана(ов) по обеспечению непрерывности служебной деятельности необходимо указывать, как и когда следует тестировать каждый пункт плана. Отдельные пункты плана(ов) необходимо тестировать часто.

Следует использовать различные методы для обеспечения уверенности в том, что план(ы) будет(ут) действовать в реальной жизни. К таким методам относятся:

а) теоретическая проверка различных сценариев (обсуждение мер по восстановлению служебной деятельности на различных примерах прерываний);

б) моделирование особенно для тренинга сотрудников по выполнению их ролей управления в постинцидентных и кризисных ситуациях;

в) тестирование технического восстановления (обеспечение уверенности в возможности эффективного восстановления систем);

г) тестирование процессов восстановления деятельности на альтернативной площадке (процессы служебной деятельности осуществляются параллельно с процедурами восстановления на удаленной альтернативной площадке);

д) тестирование оборудования и услуг поставщиков (обеспечение уверенности в том, что предоставленные сторонними орган внутренних дел продуктами и услуги удовлетворяют договорным обязательствам);

е) «генеральные репетиции» (проверка готовности персонала, оборудования, средств и процессов к обеспечению непрерывности служебной деятельности).

Указанные методы могут использоваться любым органом внутренних дел. Они должны применяться в соответствии со спецификой конкретного плана по восстановлению. Результаты тестов следует регистрировать и при необходимости осуществлять действия, направленные на совершенствование планов.

Необходимо назначить ответственных за проведение регулярных пересмотров каждого плана по обеспечению непрерывности служебной деятельности. Выявление изменений в процессах

служебной деятельности, еще не отраженных в планах по обеспечению непрерывности служебной деятельности, должно сопровождаться соответствующим обновлением планов. Указанный формальный процесс управления изменениями призван обеспечить уверенность в том, что обновленные планы распространяются и подкрепляются в соответствии с регулярным пересмотром комплексного плана.

Примеры ситуаций, которые могли бы потребовать обновления планов по обеспечению непрерывности служебной деятельности, включают приобретение нового оборудования или обновления систем, а также изменения, связанные с:

- а) персоналом;
- б) адресами или номерами телефонов;
- в) стратегией служебной деятельности;
- г) местоположением, условиями и ресурсами;
- д) законодательством;
- е) подрядчиками, поставщиками и основными клиентами;
- ж) процессами, как новыми, так упраздненными;
- з) рисками (эксплуатационными и финансовыми).

11.2. Соответствие требованиям нормативных правовых актов

Цель: Избежать нарушений любого закона, правовых, нормативных или договорных обязательств, а также любых требований безопасности.

Проектирование, функционирование, использование информационных систем и управление ими может быть предметом применения правовых, нормативных и договорных требований безопасности.

Следует консультироваться с юрисконсультom органа внутренних дел в отношении конкретных юридических вопросов, или с практикующими юристами, имеющими соответствующую квалификацию. Законодательные требования разных стран отличаются друг от друга, и они могут меняться в отношении информации, созданной в одной стране и переданной в другую страну (например, информационный поток, передаваемый через границу).

11.2.1. Определение применимого законодательства

Все применимые правовые, нормативные и договорные требования и подходы органа внутренних дел к выполнению этих требований следует четко определить, документально оформить и поддерживать на актуальном уровне в отношении каждой информационной системы и органа внутренних дел.

Конкретные меры и средства контроля и управления, а также обязанности конкретных лиц по выполнению этих требований необходимо определить и документально оформить.

11.2.2. Права на интеллектуальную собственность

Необходимо внедрить соответствующие процедуры для обеспечения уверенности в соблюдении законодательных, нормативных и договорных требований по использованию материалов, в отношении которых могут иметься права на интеллектуальную собственность, и по использованию проприетарных программных продуктов.

Проприетарное программное обеспечение:

- программное обеспечение, защищенное авторским/патентным правом. Модификация и дальнейшее распространение такого программного обеспечения запрещена или строго ограничена;
- программы собственного производства, разработанные органом внутренних дел для внутреннего использования (в отличие от стандартных программных средств известных производителей).

Следующие рекомендации следует учитывать в отношении защиты любого материала, который может рассматриваться как интеллектуальная собственность:

- а) создание политики соблюдения прав на интеллектуальную собственность в отношении программного обеспечения, определяющей законное использование программных и информационных продуктов;
- б) приобретение программного обеспечения только из известных и заслуживающих доверия источников для обеспечения уверенности в том, что авторское право не нарушается;

в) поддержание осведомленности сотрудников о политиках по защите прав на интеллектуальную собственность и уведомление о намерении применить дисциплинарные санкции в отношении нарушителей;

г) поддержание соответствующих реестров активов и выявление всех активов, в отношении которых применимы требования по защите прав на интеллектуальную собственность;

д) сохранение подтверждений и свидетельств прав собственности на лицензии, дистрибутивные диски, руководства по эксплуатации и т. д.;

е) внедрение мер и средств контроля и управления для обеспечения уверенности в том, что максимальное число разрешенных пользователей не превышено;

ж) проведение проверок на предмет установки только авторизованного программного обеспечения и лицензированных продуктов;

з) предоставление политики по поддержке условий соответствующих лицензионных соглашений;

и) предоставление политики утилизации или передачи программного обеспечения другим сторонним организациям;

к) использование соответствующих инструментальных средств аудита;

л) соблюдение сроков и условий применения программного обеспечения и информации, полученной из общедоступных сетей;

м) запрещать дублирование, преобразование или извлечение из коммерческих записей (видео, аудио) с нарушением закона об авторском праве;

н) запрещать полное или частичное копирование книг, статей, отчетов или других документов с нарушением закона об авторском праве.

Права на интеллектуальную собственность охватывают авторское право на программное обеспечение или документы, права на проекты, торговые марки, патенты и лицензии на исходные тексты программ.

Проприетарные программные продукты обычно поставляются в соответствии с лицензионным соглашением, которое определяет права по срокам и условиям использования, например ограничение на использование продуктов



в указанных компьютерах или ограничение копирования только созданием резервных копий. Ситуацию в отношении прав на интеллектуальную собственность в отношении программного обеспечения, разработанного орган внутренних дел, следует разъяснить персоналу.

Законодательные, нормативные и договорные требования могут вводить ограничения на копирование материалов, являющихся предметом собственности. В частности, данные ограничения могут содержать требования на использование только тех материалов, которые или разработаны органом внутренних дел, или представлены по лицензии, или переданы разработчиками для органа внутренних дел. Нарушение авторского права может привести к судебному иску, который может повлечь уголовное преследование.

11.2.3. Предотвращение нецелевого использования средств обработки информации

Пользователей следует удерживать от применения средств обработки информации для несанкционированных целей.

Руководство должно санкционировать использование средств обработки информации. Любое использование этих средств для неслужебных целей без одобрения руководства или для каких-либо несанкционированных целей следует рассматривать как нецелевое. Если какие-либо несанкционированные действия определяются мониторингом или другими средствами, то на них следует обратить внимание непосредственного руководителя сотрудника, с целью принятия соответствующих мер дисциплинарного и (или) правового воздействия.

Прежде чем осуществлять процедуры мониторинга, необходимо получить консультацию юрисконсульта.

Все пользователи должны быть осведомлены о четких рамках разрешенного им доступа и о проведении мониторинга с целью обнаружения несанкционированного использования средств обработки информации. Это может быть достигнуто путем предоставления пользователям письменного разрешения, копия которого должна быть подписана пользователем и надежно хра-

ниться в органе внутренних дел. Необходимо, чтобы сотрудники органа внутренних дел, подрядчики и представители сторонней орган внутренних дел были осведомлены о том, что никакой доступ не разрешен, за исключением того, который авторизован.

Необходимо, чтобы при начале сеанса на экране компьютера было представлено предупреждающее сообщение, указывающее, что средство обработки информации, вход в которое пытаются осуществить, является собственностью орган внутренних дел, и что несанкционированный доступ к нему запрещен. Пользователь должен подтвердить прочтение и соответствующим образом реагировать на это сообщение на экране, чтобы продолжить процесс начала сеанса.

Средства обработки информации органа внутренних дел должны использоваться главным образом только для решения задач служебной деятельности.

Обнаружение вторжения, проверка содержания и другие средства мониторинга могут помочь в предотвращении и обнаружении нецелевого использования средств обработки информации.

Во многих странах введено законодательство, касающееся защиты от неправильного использования компьютеров. Использование компьютера для несанкционированных целей может расцениваться как уголовное преступление.

Законность проведения мониторинга в отношении использования средств обработки информации зависит от страны, и может потребоваться, чтобы сотрудники были уведомлены о таком мониторинге и (или) чтобы было получено их согласие. При осуществлении входа в систему, используемую для открытого доступа (например, общественный Web-сервер) и подвергаемую мониторингу безопасности, на экране компьютера должно отображаться сообщение, информирующее об этом.



ЗАКЛЮЧЕНИЕ

В учебном пособии даны понятийный аппарат и основы управления информационной безопасностью органов внутренних дел Российской Федерации. Изложены организационные аспекты управления информационной безопасностью. Рассмотрены вопросы управления рисками информационной безопасности. Представлены наиболее важные аспекты управления инцидентами информационной безопасности.

Также в пособии приведены и глубоко рассмотрены следующие вопросы:

- общие положения и нормативно-правовое регулирование управления информационной безопасностью;
- организационные аспекты управления информационной безопасностью;
- управление рисками информационной безопасности
- управление информационными активами;
- управление персоналом;
- управление физической безопасностью;
- управление информационной безопасностью при использовании средств коммуникации;
- управление доступом к информационным активам;
- управление информационной безопасностью при приобретении, разработке и эксплуатации информационных систем;
- управление инцидентами информационной безопасности;
- управление непрерывностью деятельности.

Данное учебное пособие может быть также использовано на занятиях в системе служебной подготовки и для профессиональной подготовки сотрудников подразделений информационных технологий, связи и защиты информации территориальных органов МВД России.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 27000-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

2. ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

3. ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

4. ГОСТ Р ИСО/МЭК 27003-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

5. ГОСТ Р ИСО/МЭК 27004-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

6. ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

7. ГОСТ Р ИСО/МЭК 27006-2008. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ин-

формационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

8. ГОСТ Р ИСО/МЭК 27007-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

9. ГОСТ Р ИСО/МЭК 27011-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

10. ГОСТ Р ИСО/МЭК 27031-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности служебной деятельности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

11. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

12. ГОСТ Р ИСО/МЭК 27033-2-2012. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

13. ГОСТ Р ИСО/МЭК 27033-3-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

14. ГОСТ Р ИСО/МЭК 27034-1-2014. Национальный стандарт Российской Федерации. Информационная технология.

Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

15.ГОСТ Р ИСО/МЭК 27037-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

16.ГОСТ Р ИСО/МЭК 27038-2016. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Требования и методы электронного цензурирования. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

17.ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

18.ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

19.ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

20.ГОСТ Р ИСО 10007-2007. Менеджмент организации. Руководящие указания по управлению конфигурацией. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

21.ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

22.ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. // СПС «КонсультантПлюс». – Режим доступа: <http://www.consultant.ru>.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	3
1. ОБЩИЕ ПОЛОЖЕНИЯ И НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.....	6
1.1. Основные термины и определения в области управления информационной безопасностью.....	6
1.2. Нормативно-правовое регулирование управления информационной безопасностью.....	10
1.2.1. Стандарты в области управления информационной безопасностью, используемые в Российской Федерации	10
1.2.2. Международные стандарты в области управления информационной безопасностью.....	12
2. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.....	15
2.1. Политика информационной безопасности.....	15
2.1.1. Документирование политики информационной безопасности.....	15
2.1.2. Пересмотр политики информационной безопасности.....	17
2.2. Организационные аспекты информационной безопасности.....	18
2.2.1. Обязательства руководства по отношению к информационной безопасности.....	19
2.2.2. Координация вопросов информационной безопасности.....	20
2.2.3. Распределение обязанностей по обеспечению информационной безопасности.....	21
2.2.4. Процесс получения разрешения на использование средств обработки информации.....	22
2.2.5. Соглашения о конфиденциальности.....	22
2.2.6. Контакт с различными инстанциями.....	24
2.2.7. Контакт со специализированными профессиональными группами.....	24
2.2.8. Независимая проверка информационной безопасности.....	25
2.3. Аспекты взаимодействия со сторонними организациями.....	26

2.3.1. Идентификация рисков, являющихся следствием работы со сторонними организациями.....	27
2.3.2. Рассмотрение требований безопасности в договорах с третьей стороной.....	30
2.3. Процессный подход.....	33
2.4. Система управления информационной безопасностью.....	36
2.4.1. Разработка системы управления информационной безопасностью.....	36
2.4.2. Внедрение и функционирование системы управления информационной безопасностью.....	38
2.4.3. Проведение мониторинга и анализа системы управления информационной безопасностью.....	39
2.4.4. Поддержка и улучшение системы управления информационной безопасностью.....	40
3. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	41
3.1. Основные варианты стратегии анализа рисков информационной безопасности органа внутренних дел.....	41
3.1.1. Базовый подход.....	43
3.1.2. Неформальный подход.....	44
3.1.3. Детальный анализ риска.....	45
3.1.4. Комбинированный подход.....	46
3.2. Управление рисками информационной безопасности.....	51
3.2.1. Установление границ рассмотрения.....	53
3.2.2. Идентификация активов.....	54
3.2.3. Оценка активов и установление зависимости между активами.....	55
3.2.4. Оценка угроз.....	58
3.2.5. Оценка уязвимости.....	60
3.2.6. Идентификация существующих/планируемых защитных мер.....	62
3.2.7. Оценка рисков.....	62
3.3. Выбор защитных мер.....	63
3.3.1. Определение защитных мер.....	64
3.3.2. Структура безопасности информационных технологий.....	68
3.3.3. Идентификация и анализ ограничений.....	70
3.4. Приемлемость рисков.....	72

4. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ АКТИВАМИ.....	73
4.1. Ответственность за активы.....	73
4.1.1. Инвентаризация активов.....	73
4.1.2. Владение активами.....	74
4.1.3. Приемлемое использование активов.....	75
4.2. Классификация информации.....	76
4.2.1. Рекомендации по классификации.....	76
4.2.2. Маркировка и обработка информации.....	77
5. УПРАВЛЕНИЕ ПЕРСОНАЛОМ.....	79
5.1. Перед трудоустройством.....	79
5.1.1. Роли и обязанности.....	79
5.1.2. Предварительная проверка.....	80
5.1.3. Условия занятости.....	81
5.2. В течение занятости.....	83
5.2.1. Обязанности руководства.....	83
5.2.2. Осведомленность, обучение и тренинг в области информационной безопасности.....	85
5.2.3. Дисциплинарный процесс.....	86
5.3. Прекращение или смена занятости.....	86
5.3.1. Прекращение обязанностей.....	87
5.3.2. Возврат активов.....	88
5.3.3. Аннулирование прав доступа.....	88
6. УПРАВЛЕНИЕ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТЬЮ	90
6.1. Зоны безопасности.....	90
6.1.1. Периметр зоны безопасности.....	90
6.1.2. Меры и средства контроля и управления физическим входом.....	92
6.1.3. Безопасность зданий, служебных помещений и оборудования.....	93
6.1.4. Защита от внешних угроз и угроз со стороны окружающей среды.....	93
6.1.5. Работа в зонах безопасности.....	94
6.1.6. Зоны общего доступа, приемки и отгрузки.....	95
6.2. Безопасность оборудования.....	95
6.2.1. Размещение и защита оборудования.....	96
6.2.2. Поддерживающие услуги.....	97
6.2.3. Безопасность кабельной сети.....	98

6.2.4. Техническое обслуживание оборудования.....	99
6.2.5. Безопасность оборудования вне помещений органа внутренних дел.....	100
6.2.6. Безопасная утилизация или повторное использование оборудования.....	101
6.2.7. Перемещение имущества.....	102
7. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ КОММУНИКАЦИИ.....	103
7.1. Эксплуатационные процедуры и обязанности.....	103
7.1.1. Документальное оформление эксплуатационных процедур.....	103
7.1.2. Управление изменениями.....	104
7.1.3. Разделение обязанностей.....	105
7.1.4. Разделение средств разработки, тестирования и эксплуатации.....	106
7.2. Управление оказанием услуг третьей стороной.....	108
7.2.1. Предоставление услуг.....	108
7.2.2. Мониторинг и анализ услуг третьей стороны.....	108
7.2.3. Управление изменениями услуг третьей стороны	110
7.3. Планирование и приемка систем.....	111
7.3.1. Управление производительностью.....	111
7.3.2. Приемка систем.....	112
7.4. Защита от вредоносных и мобильных программ....	113
7.4.1. Меры и средства контроля и управления против вредоносной программы.....	113
7.4.2. Меры и средства контроля и управления при использовании мобильной программы.....	116
7.5. Резервирование.....	117
7.6. Управление безопасностью сети.....	118
7.6.1. Меры и средства контроля и управления сетями..	119
7.6.2. Безопасность сетевых услуг.....	120
7.7. Обращение с носителями информации.....	121
7.7.1. Управление сменных носителей информации.....	121
7.7.2. Утилизация носителей информации.....	122
7.7.3. Процедуры обработки информации.....	123
7.7.4. Безопасность системной документации.....	124
7.8. Обмен информацией.....	124
7.8.1. Политики и процедуры обмена информацией.....	125
7.8.2. Соглашения по обмену информацией.....	128

7.8.3. Физические носители информации при транспортировке.....	129
7.8.4. Электронный обмен сообщениями.....	130
7.8.5. Информационные системы служебной деятельности.....	131
7.9. Мониторинг.....	132
7.9.1. Контрольная регистрация.....	132
7.9.2. Использование системы мониторинга.....	133
7.9.3. Защита информации журналов регистрации.....	135
7.9.4. Журналы регистрации администратора и оператора.....	135
7.9.5. Регистрация неисправностей.....	136
7.9.6. Синхронизация часов.....	137
8. УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ АКТИВАМ.....	138
8.1. Требования служебной деятельности по управлению доступом.....	138
8.1.1. Политика управления доступом.....	138
8.2. Управление доступом пользователей.....	140
8.2.1. Регистрация пользователей.....	140
8.2.2. Управление привилегиями.....	141
8.2.3. Управление паролями пользователей.....	142
8.2.4. Пересмотр прав доступа пользователей.....	143
8.3. Обязанности пользователя.....	144
8.3.1. Использование паролей.....	144
8.3.2. Оборудование пользователя, оставленное без присмотра.....	146
8.3.3. Политика «чистого стола» и «чистого экрана»....	146
8.4. Управление доступом к сети.....	148
8.4.1. Политика использования сетевых услуг.....	148
8.4.2. Аутентификация пользователей для внешних соединений.....	149
8.4.3. Идентификация оборудования в сетях.....	151
8.4.4. Защита портов дистанционной диагностики и конфигурации.....	151
8.4.5. Разделение в сетях.....	152
8.4.6. Управление сетевыми соединениями.....	154
8.4.7. Управление сетевой маршрутизацией.....	154

8.5. Управление доступом к эксплуатируемой системе..	155
8.5.1. Безопасные процедуры начала сеанса.....	156
8.5.2. Идентификация и аутентификация пользователя..	157
8.5.3. Система управления паролями.....	158
8.5.4. Использование системных утилит.....	159
8.5.5. Лимит времени сеанса связи.....	160
8.5.6. Ограничения времени соединения.....	160
8.6. Управление доступом к информации и прикладным программам.....	161
8.6.1. Ограничение доступа к информации.....	162
8.6.2. Изоляция чувствительных систем.....	162
8.7. Мобильная вычислительная техника и дистанционная работа.....	163
8.7.1. Мобильная вычислительная техника и связь.....	164
8.7.2. Дистанционная работа.....	166
9. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ ПРИОБРЕТЕНИИ, РАЗРАБОТКЕ И ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ.....	168
9.1. Требования безопасности информационных систем	168
9.1.1. Анализ требований безопасности и спецификация.....	168
9.2. Корректная обработка в прикладных программах...	169
9.2.1. Подтверждение корректности входных данных.....	170
9.2.2. Управление внутренней обработкой.....	171
9.2.3. Целостность сообщений.....	172
9.2.4. Подтверждение выходных данных.....	173
9.3. Криптографические меры и средства контроля и управления.....	173
9.3.1. Политика использования криптографических мер и средств контроля и управления.....	174
9.3.2. Управление ключами.....	175
9.4. Безопасность системных файлов.....	177
9.4.1. Управление эксплуатируемым программным обеспечением.....	177
9.4.2. Защита тестовых данных системы.....	179
9.4.3. Управление доступом к исходным текстам программ.....	180
9.5. Безопасность в процессах разработки и поддержки.	181
9.5.1. Процедуры управления изменениями.....	181

9.5.2. Техническая проверка прикладных программ после изменений эксплуатируемой системы.....	183
9.5.3. Ограничения на изменения пакетов программ.....	184
9.5.4. Утечка информации.....	185
9.5.5. Аутсорсинг разработки программного обеспечения.....	186
9.6. Управление техническими уязвимостями.....	186
10. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	189
10.1. Оповещение о событиях и уязвимостях информационной безопасности.....	189
10.1.1. Оповещение о событиях информационной безопасности.....	189
10.1.2. Оповещение об уязвимостях безопасности.....	192
10.2. Управление инцидентами информационной безопасности и необходимое совершенствование.....	192
10.2.1. Обязанности и процедуры.....	193
10.2.2. Извлечение уроков из инцидентов информационной безопасности.....	195
10.2.3. Сбор доказательств.....	195
11. УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ ДЕЯТЕЛЬНОСТИ.....	198
11.1. Аспекты информационной безопасности в рамках управления непрерывностью служебной деятельности.....	198
11.1.1. Включение информационной безопасности в процесс управления непрерывностью служебной деятельности.....	199
11.1.2. Непрерывность служебной деятельности и оценка риска.....	200
11.1.3. Разработка и внедрение планов обеспечения непрерывности служебной деятельности, учитывающих информационную безопасность.....	201
11.1.4. Основы планирования непрерывности служебной деятельности.....	203
11.1.5. Тестирование, поддержка и пересмотр планов непрерывности служебной деятельности.....	204
11.2. Соответствие требованиям нормативных правовых актов.....	206

11.2.1. Определение применимого законодательства....	207
11.2.2. Права на интеллектуальную собственность.....	207
11.2.3. Предотвращение нецелевого использования средств обработки информации.....	209
ЗАКЛЮЧЕНИЕ.....	211
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	212

Учебное издание

**УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ**

Учебное пособие

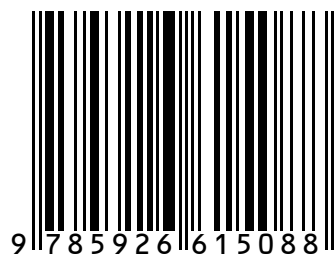
Составители:

Клюев Станислав Геннадьевич
Сизоненко Александр Борисович

В авторской редакции

Компьютерная верстка *С. В. Коноваловой*

ISBN 978-5-9266-1508-8



Подписано в печать 23.10.2019. Формат 60х84 1/16.
Усл. печ. л. 12,5. Тираж 100 экз. Заказ 839.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.