УДК 006.032

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Шилов А.К., Мищенко В.И.

ФГАОУ ВО «Инженерно-технологическая академия Южного федерального университета», Таганрог, e-mail: vovchikcool@inbox.ru

Рассмотрен основной американский стандарт в области безопасности государственных информационных систем. Описываются главные принципы и выбор базовых мер безопасности. Данный стандарт предназначен, чтобы служить разнообразной аудитории профессионалов по информационным системам и информационной безопасности.

Ключевые слова: государственная информационная система (ГИС), доверие, информационная безопасность, управления рисками, меры безопасности, требования безопасности, оверлей

SECURITY OF INFORMATION IN GOVERNMENT INFORMATION SYSTEMS

Shilov A.K., Mishchenko V.I.

Engineering Academy of Southern Federal University, Taganrog, e-mail: vovchikcool@inbox.ru

We considered the basic American standard in security of government information systems. Describes the main principles and basic choices of security measures. This standard is intended to serve a diverse audience of professionals in information systems and information security.

Keywords: government information system (GIS), trust, information security, risk management, safety measures, safety requirements, overlay

Информационная безопасность является важной составляющей любой компании, любого предприятия. Для ее обеспечения требуется отличное знание построения системы защиты, документации, стандартов. Как правило в защите нуждаются информационные системы. Основной же для государства является государственная информационная система. Публикация NIST Special Publication 800-53. Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations обеспечивает каталог мер обеспечения безопасности и приватности для федеральных информационных систем и организаций и процесса выбора мер безопасности для защиты деятельности организаций (включая предназначение, функции, имидж и репутацию), активов, организаций, людей, других организаций от набора разнообразных угроз, включая враждебные кибератаки, стихийные бедствия, структурные отказы и человеческие ошибки. Меры обеспечения адаптируются и реализуются как часть общего для организации процесса, который управляет информационными рисками безопасности и приватности. Меры обеспечения определяются разнообразным набором требований безопасности и приватности для федерального правительства и критической инфраструктуры, полученных из законодательства, правительственных распоряжений, политик, директив, постановлений, стандартов и/или потребностей предназначения и деятельности. Публикация также описывает, как разработать специализированные наборы мер обеспечения или оверлеи, адаптированные для определенных типов функций предназначения/деятельности, технологий или сред эксплуатации.

Основные принципы

Информационная система – это комплекс, который включает компьютерное и коммуникационное оборудование, программное обеспечение, информационные ресурсы, а также системный персонал [1]. Государственные информационные системы же – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ, на основании правовых актов государственных органов.

Есть несколько ключевых вопросов, на которые должны ответить организации, когда рассматривают информационную безопасность для информационных систем:

- Какие меры безопасности необходимы, чтобы удовлетворить требованиям безопасности и соответственно смягчить риск, существующий при использовании информации и информационных систем в выполнении задач и коммерческих функций организаций?
- Реализованы ли меры безопасности или существует ли план их реализации?
- Каков желаемый или требуемый уровень доверия, что выбранные меры безопасности, при реализации, были эффективны в их применении?

Публикация представляет фундаментальные концепции, связанные с выбором

и спецификацией мер безопасности включая: трехуровневое управление рисками, структуру мер безопасности и их организация в каталоге мер безопасности, базовые меры безопасности, идентификацию и использование мер обеспечения коллективной безопасности, меры безопасности во внешних средах, меры доверия к безопасности и будущие версии мер безопасности, каталога мер и базовых мер безопасности [2].

Выбор базовых наборов мер безопасности

При подготовке к выбору и определению надлежащих мер безопасности для информационных систем организаций и соответствующих сред эксплуатации, организации сначала определяют критичность и чувствительность информации, которая будет обрабатываться, храниться или передаваться этими системами. Обобщенный формат для того, чтобы определить категорию безопасности (SC) информационной системы следующий:

$\mathbf{SC}_{\text{Информационная система}}$ = {(**конфиденциальность**, *воздействие*), (**целостность**, *воздействие*), (**доступность**, *воздействие*)}, где приемлемые значения для потенциального воздействия низко, умеренно или высоко.

Для определения уровня воздействия для информационной системы следует:

1. Определить различные типы информации, которые обрабатываются, хранятся или передаются информационной системой.

2. Разделить на категории конфиденциальность, целостность и доступность для каждого типа информации.

3. Провести категорирование безопасности информационной системы, то есть, определить самые высокие значения воздействий для каждой цели безопасности (конфиденциальности, целостности, доступности) из числа категорированных для типов информации, связанных с информационной системой.

4. Определить полный уровень воздействия для информационной системы как самого высокого значения воздействия среди трех целей безопасности в категорировании безопасности системы.

После выбора применимого базового набора мер безопасности из организации инициируют процесс адаптации, чтобы соответственно изменить и выровнять меры безопасности более близко с особыми условиями в организациях (то есть, условиями, связанными с функциями предназначения деятельности, информационными системами или средами эксплуатации организаций). Процесс адаптации включает:

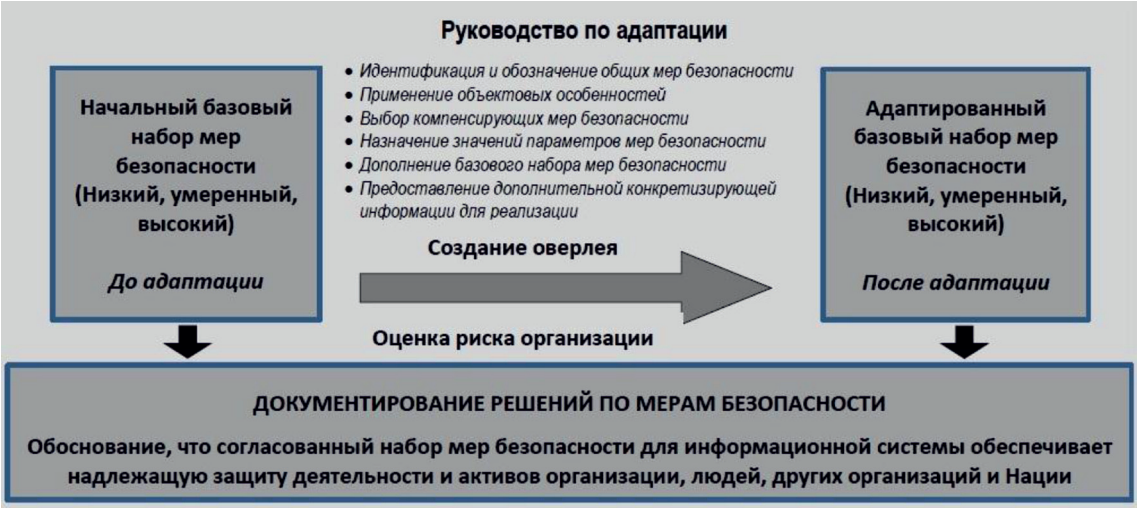
- идентификацию и определение общих мер безопасности в начальных базовых наборах мер безопасности;
- применение объектовых особенностей к остальным мерам базового набора мер безопасности;
- выбор компенсирующих мер безопасности, если необходимо;
- назначение конкретных значений для определенных организациями параметров мер безопасности через операции явного назначения и выбора;
- дополнение базовых наборов дополнительными мерами безопасности и улучшениями мер безопасности, если необходимо;
- предоставление дополнительной специфичной информации для реализации мер безопасности, если необходимо.

Процесс адаптации, как неотъемлемая часть выбора и спецификации мер безопасности, является частью всестороннего процесса управления рисками организации – структурирования, оценки, реакции на и мониторинга риска информационной безопасности. Организации используют руководство управления рисками, чтобы облегчить основанное на риске принятие решений относительно применимости мер безопасности в базовых наборах мер безопасности. В конечном счете, организации используют процесс адаптации, чтобы достигнуть рентабельной, основанной на риске безопасности, которая поддерживает потребности предназначения/деятельности организаций.

Для учета потребности в разработке наборов мер безопасности для информационных систем и организаций, предназначенных для сообществ и специализированных, введена концепция оверлея. Оверлей – полностью определенный набор мер безопасности, улучшений мер и дополнительное руководство. Оверлеи дополняют начальные базовые наборы мер безопасности: обеспечивая возможность добавить или устранить меры безопасности; обеспечивая применимость мер безопасности и интерпретации для конкретных информационных технологий, вычислительных парадигм, сред эксплуатации, типов информационных систем, типов предназначений/деятельности, рабочих режимов, отраслевых секторов и законодательных/нормативных требований; устанавливая для сообществ значения параметров для операций назначения и/или выбора в мерах безопасности и улучшениях мер; и расширяя дополнительное руководство для мер безопасности, где необходимо. Организации, как правило, используют концепцию оверлея, когда есть расхождение с основными предположениями,

использованными при создании начальных базовых наборов мер безопасности.

Организации документируют соответствующие решения, принятые в процессе выбора мер безопасности, давая разумное обоснование этих решений. Эта документация важна, когда исследуются соображения безопасности для информационных систем организаций относительно потенциального влияния на их назначение/ деятельность. Результирующий набор мер и поддерживающее обоснование для выбранных решений (включая любые используемые ограничения для информационных систем, требуемые организациями) документируются в планы обеспечения безопасности. Документирование существенных решений управления рисками в процессе выбора мер безопасности обязательно делать так, чтобы у санкционирующих должностных лиц мог быть доступ к необходимой информации, чтобы сделать осмысленные решения по санкционированию для информационных систем организации. Без такой информации, понимание, предположений, ограничений и обоснования, поддерживающего эти решения управления рисками, по всей вероятности, не будет доступно, когда состояние информационных систем или среды эксплуатации изменится, и исходные решения риска будут пересматриваться. Рисунок суммирует процесс выбора мер безопасности, включая выбор начального базового набора мер безопасности и адаптацию базового набора:



Процесс выбора мер безопасности

Заключение

Рассматриваемый документ интересен тем, что в последнее время он активно внедряется в информационную среду многих предприятий, хоть и является американским стандартом. Наконец, каталог мер безопасности определяет безопасность и с точки зрения функциональности (обеспечиваемой стойкостью функций и механизмов безопасности) и с точки зрения доверия (мер уверенности в реализованных возможностях безопасности). Обеспечение и функциональности безопасности и доверия к безопасности гарантирует, что продукты информационных технологий и информационные системы, созданные из этих продуктов, используя системные и инженерные принципы обеспечения безопасности, будут достаточно надёжны.

Список литературы

1. Титоренко Г.А. Информационные системы в экономике. – М.: ЮНИТИ-ДАНА, 2008. – С. 16.

2. NIST Special Publication 800-53. Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2013. – 457 p.