УДК 004.01
DOI 10.33764/2618-981X-2022-6-116-121

Нормативная база для формирования системы информационной безопасности ядерного объекта

Е. А. Кузнецова[1], А. Н. Фионов[2]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация

[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация

* e-mail: elizaveta.kuznetsova04@mail.ru

Аннотация. Уязвимость ядерных объектов к преднамеренному нападению вызывает озабоченность в области обеспечения ядерной безопасности. Ведь большинство ядерных объектов уязвимы для атак, которые могут привести к масштабному радиоактивному загрязнению и массовой гибели людей. Если использование ядерной энергии со временем должно значительно увеличиться, то ядерные объекты должны быть защищены от атак, которые в последствии могут выбросить большое количество отходов. В данной статье будут рассмотрены основные нормативные документы, которые будут являться основой для формирования системы информационной безопасности ядерных объектов. Целью работы является анализ нормативной базы в области информационной безопасности применительно к объектам, реализующим различные ядерные технологии. Задача – выработка технических требований к системам обеспечения информационной безопасности, учитывающих специфику таких объектов.

Ключевые слова: информационная безопасность, ядерный объект, криптографическая защита информации

Regulatory framework for the formation of the system information security of a nuclear facility

E. A. Kuznetsova[1], A. N. Fionov[2]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

[2] Siberian State University of telecommunications and computer science, Novosibirsk, Russian Federation

* e-mail: elizaveta.kuznetsova04@mail.ru

Abstract. The vulnerability of nuclear facilities to deliberate attack raises concerns in the field of nuclear safety. After all, most nuclear facilities are vulnerable to attacks that can lead to widespread radioactive contamination. If the use of nuclear energy is to expand significantly, nuclear facilities must be extremely protected from attacks that can release huge amounts of radioactivity into the community. This article will consider the main regulatory documents that will be the basis for the formation of an information security system for nuclear facilities. The purpose of the work is to analyze the regulatory framework in the field of information security in relation to facilities implementing various nuclear technologies. The task is to develop technical requirements for information security systems that take into account the specifics of such objects.

Keywords: information security, nuclear facility, cryptographic protection of information

Введение

Значение информационной безопасности в Российской Федерации только возрастает, так как это одна из главных составляющих национальной безопасности. Применение средств обеспечения информационной безопасности зарубеж-

ного производства содержит в себе значительные угрозы для России и ее граждан, особенно в области информационных технологий. Основное направление обеспечения национальной безопасности России – это разработка и создание доверенных отечественных технологий и средств защиты информации. Основными регуляторами в России в области защиты информации являются органы исполнительной власти ФСТЭК и ФСБ России, каждый в пределах своих полномочий [1]. Органами ФСБ осуществляется государственный контроль за организацией и работой криптографической безопасности информационных систем, сетей связи, которые обеспечивают передачу информации с использованием шифров, а ФСТЭК в свою очередь осуществляет реализацию государственной политики, организовывает межведомственную координации и взаимодействие, специальные и контрольные функции в области государственной безопасности.

Криптографические методы занимают особое место в обеспечении информационной безопасности. На базе научной криптографической школы России успешно развивается отрасль промышленности по разработке и созданию криптографической техники для обеспечения информационной безопасности. Так как рассматривается нормативная база для защиты ядерных объектов, то согласно проведенному исследованию можно выделить два основных типа: объекты ядерной энергетики (АЭС) и научно-исследовательские организации, работающие в сфере ядерных технологий.

Задачи обеспечения информационной безопасности в этих типах объектов существенно различаются. АЭС работает в замкнутом технологическом цикле и, в принципе, все информационные процессы, связанные с управлением технологией, могут быть замкнуты внутри объекта, т.е. отсутствует внешний нарушитель. Примерами таких объектов являются атомные электростанции и научно-исследовательские организации, имеющие ядерные реакторы и работающие с радиоактивными веществами. В действующих нормативных документах в области информационной безопасности такие объекты явно не выделяются [2].

Однако такие прецеденты, как авария на Чернобыльской АЭС, говорят о необходимости внешнего мониторинга деятельности персонала и состояния критических узлов, что требует организации информационного обмена с внешними агентами. В научно-исследовательских организациях ситуация еще более усложняется, так как требуется совмещать достаточно открытый информационный обмен по линии научных исследований и разработок с управлением опасными установками. Особое значение представляет разработка средств защиты информации для объектов, использующих ядерные технологии.

Поэтому цель настоящей статьи заключается в формулировании требований к системам обеспечения информационной безопасности ядерных объектов на основе действующих в РФ нормативно-технических документов. Это позволит сформулировать требования к технической реализации системы защиты [3].

Методы и методология

Для создания технических требований к системам обеспечения информационной безопасности ядерных объектов необходимо проанализировать нормативные документы, относящиеся к теме нашего исследования. В данном случае мы

рассмотрим стандарты средств криптографической защиты информации (СКЗИ), разработкой которых занимается технический комитет (ТК) № 26. Технический комитет занимается объектами стандартизации, к которым относятся методы шифрования информации, способы их реализации, а также методы обеспечения безопасности информационных технологий, которые используют криптографические преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись [4].

В первую очередь выделим Р 1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня» и поправка к Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования» из рекомендаций СКЗИ технического комитета 26 [5,6]. Помимо стандартов, разрабатываемых ТК 26, для создания технических требований нам понадобится следующий перечень нормативных документов:

– Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» [7];

– Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями и дополнениями) [8];

– Постановление Правительства РФ от 16 апреля 2012 г. N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных ...» [9].

Результаты

На основании анализа данной нормативной документации выделены определенные требования, касающиеся информационной безопасности ядерных объектов.

Данными требованиями являются:

1. Требования к СКЗИ:

– обработка, хранение и передача по каналам связи информации, включая СКЗИ, обеспечивается безопасностью;

– информация обеспечивается безопасностью от несанкционированного доступа к информации при ее обработке и хранении;

– безопасность информации обеспечивается от навязывания ложной информации, включая средства имитозащиты и «электронной подписи».

2. Требования к безопасности конфиденциальной информации:

– сотрудниками органов криптографической защиты информации должна соблюдаться конфиденциальность при обращении с данными, которые им доверены или стали известны по работе;

– сотрудниками органов криптографической защиты должны выполняться требования, обеспечивающие безопасность конфиденциальной информации;

– сотрудники органов криптографической защиты должны надежно хранить СКЗИ, техническую документацию, ключевые документы, носители конфиденциальной информации;

– сотрудники органов криптографической защиты должны своевременно выявлять посторонних лиц при попытке получения сведений о защищаемой конфиденциальной информации;

– сотрудники органов криптографической защиты должны немедленно принимать меры по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ.

3. Требования к сотрудникам, использующим СКЗИ:

– сотрудники не в праве разглашать конфиденциальную информацию, к которой они допущены;

– соблюдение требований к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

– сотрудники обязаны сообщать в органы криптографической защиты о попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– органы криптографической защиты должны быть немедленно уведомлены о фактах утраты или недостачи СКЗИ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки сведений.

4. Требования к осуществлению контроля за соблюдением правил пользования СКЗИ.

Контроль осуществляется:

– пользователем защищаемой информации с применением СКЗИ;

– владельцем информационных систем с применением СКЗИ;

– ФСБ России в рамках контроля за организацией и функционированием криптографической безопасности информационных систем, систем шифрованной связи.

5. Требования к защите технических средств.

Защита от несанкционированного доступа осуществляется с помощью:

– технических средств системы, обрабатывающих информацию;

– средств, обеспечивающих функционирование системы;

– помещений, в которых средства постоянно расположены.

Также необходимо реализовать защиту технических средств от внешних деструктивных воздействий и защиту информации, предоставляемой в виде информативных электрических сигналов [10]. Помимо данных требований необходимо усилить защиту, усовершенствовать систему предупрежения чрезвычайных ситуаций и организацию аварийной готовности.

Заключение

В результате изучения различных источников сделан вывод, что требуется строить для объектов многоуровневую систему защиты информации с существенно различными мерами защиты на разных уровнях. Конкретизировали требования к системам информационной безопасности на основе имеющихся нормативно-технических документов. Сформулировали требования к технической реализации системы защиты ядерных объектов. Главная цель заключается в обеспечении надежной, безотказой работы информационнной инфраструктуры ядерного объекта в условиях внешних воздействий и внутренних атак, а также расследования подобных инцедентов и в защите конфиденциальной информации. Ведь система безопасности ядерого объекта связана с развитием компьютерных технологий и систем управления технологических процессов и управлением другими системами безопасности. Это необходимо для развития и совершенствования системы кибербезопасности ядерных объектов, так как участились кибератаки на ядерные объекты [11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Горев А. И., Симаков А. А. Обеспечение Информационной Безопасности. Москва: Мир, 2005. – 844 с.

2. Дрон К.К. О перспективах совместного использования методов квантовой и классической криптографии // Вестник Хакасского государственного университета им НФ Катанова. – 2018. – № 24. – С. 8-11.

3. Кузьмин Т. В. Криптографические методы защиты информации. Москва: Огни, 2013. – 192 с.

4. Молдовян Д. Н. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах. — URL: https://cyberleninka.ru/article/n/novaya-kontseptsiya-razrabotki-postkvantovyh-algoritmov-tsifrovoy-podpisi-na-nekommutativnyh-algebrah/viewer (дата обращения: 10.03.2022).

5. Р 1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня». – URL: http://www.consultant.ru/document/cons_doc_LAW_245704/.

6. Поправка к Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования». – URL: http://www.consultant.ru/document/cons_doc_LAW_216734/.

7. Приказ ФАПСИ «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» от 13 июня 2001 г. N 152. – URL: http://www.consultant.ru/document/cons_doc_LAW_216354/.

8. Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положе-

ние ПКЗ-2005)» (с изменениями и дополнениями) от 9 февраля 2005 г. N 66. – URL: http://www.consultant.ru/document/cons_doc_LAW_216754/.

9. Постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных...» (с изменениями и дополнениями) от 16 апреля 2012 г. N 313. – URL: http://www.consultant.ru/document/cons_doc_LAW_216704/.

10. Хоффман Л. Дж. Современные методы защиты информации. Санкт-Петербург: Питер, 2014. – 264 с.

11. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах. Москва: Горячая линия, 2012. – 322 с.