***Евстратенко Елена Сергеевна***
аспирант, ассистент
***Селифанов Валентин Валерьевич***
старший преподаватель
***Таратынова Ульяна Вадимовна***
студентка
ФГБОУ ВО «Новосибирский государственный
университет экономики и управления «НИНХ»
г. Новосибирск, Новосибирская область

# ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С УЧЕТОМ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РАЗРАБОТАННЫХ В СООТВЕТСТВИИ С ГОСТ Р ИСО/МЭК 27001

***Аннотация****: авторы статьи отмечают, что для обеспечения более продуктивной деятельности предприятия внедряются информационные системы. Внедрения способствует совершенствованию структуры потоков информации и системы документооборота, автоматизации процессов обработки данных. Аналогичная ситуация и в государственных информационных системах.*

***Ключевые слова****: информация, защита информации, система защиты информации, государственные информационные системы, политика информационной безопасности.*

В современном мире для обеспечения более продуктивной деятельности любого предприятия или организации повсеместно внедряются информационные системы. Целью этого внедрения является совершенствование структуры потоков информации и системы документооборота, автоматизация процессов обработки данных. Тоже самое можно сказать и о государственных информационных системах, используемых как в масштабах Российской Федерации, так и на отдельно взятых объектах.

В виду того, что информация, сведения, документы, содержащиеся в государственных информационных системах являются государственными информационными ресурсами (т.е. информация, содержащаяся в системе является официальной), крайне необходимо поддерживать и обеспечивать достоверность, актуальность, доступность циркулирующей информации в системе, а так же защиту указанной информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий с данной информацией.

ФСТЭК России, как федеральный орган исполнительной власти, осуществляющий реализацию государственной политики в области государственной безопасности, обладает в т.ч. следующими полномочиями: издаёт нормативные правовые акты по вопросам своей деятельности, разрабатывает и утверждает в пределах своей компетенции методические документы [2]. Основным нормативным актом, описывающим процесс создания защищенной государственной информационной системы, является приказ №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [3].

*Для построения информационных систем в защищенном исполнении на критически важных объектах, обеспечивающих контроль и управление технологическим и (или) производственным оборудованием и реализованными на нем технологическими и (или) производственными процессами, используют приказ №31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»* [4]. *Этот документ создан на основе приказа №17, развивает его перечень мер защиты восемью группами мер и в каждую из групп добавляет пункт *.0 (нулевая*

*мера) «разработка правил и процедур (политик) …». Данное требование в каждой из групп мер является обязательным для выполнения информационных систем всех классов защищенности.*

Однако, в разработанных ФСТЭК России нормативно-правовых, методических документах, не описаны вопросы построения системы менеджмента информационной безопасности в системе аттестации ФСТЭК. Данную проблему позволяют решить другие стандарты в области информационной безопасности, а именно стандарты серии 2700X.

Стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» определяет требования к системе менеджмента информационной безопасности [1]. Они не предназначены для конкретного вида деятельности предприятия, а являются универсальными для различных информационных систем, следовательно, могут применяться и в дополнение к приказу №17 ФСТЭК России [3].

Требования к системе защиты информации информационной системы формализуются и закрепляются в техническом задании на создание информационной системы (или на создание ее системы защиты) в соответствии с п.14.4 приказа [3]. Условия, которые необходимо учитывать при его оформлении, представлены в ГОСТ 34.602–89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы», ГОСТ 34.601–90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Разработка документации для информационных систем проводится в течение всех 8 стадий ее создания согласно ГОСТ 34.602–89 [6]. При выполнении каждой стадии следует руководствоваться требованиями стандартов, указанных в приложении А ГОСТ 51583–2014 [3,7].

Стадии создания системы защиты согласно ГОСТ 51583–2014 входят в комплекс следующих работ: формирование требований к системе, ее разработка (проектирование), внедрение, аттестация, сопровождение [7]. Схема построения системы менеджмента информационной безопасности в соответствии со стандартом ИСО/МЭК 27001 так же состоит из совокупности компонентов: разработка системы менеджмента, внедрение и функционирование, мониторинг и анализ, поддержка и улучшение [1]. Между этими системами можно провести взаимосвязь на каждом из этапов, что позволяет нам использовать стандарты и в совокупности при создании системы в защищенном исполнении [1; 7].

На этапе разработки системы защиты информации информационной системы, в соответствии с приказом №17 ФСТЭК России, происходит построение системы организационно-распорядительной документации рассматриваемой информационной системы (в т.ч. политик безопасности различных уровней) [3]. Для создания указанной документации имеет смысл воспользоваться стандартом ИСО/МЭК 27001 [1].

Для примера рассмотрим информационную систему со следующими характеристиками: государственную, локальную, подключенную к сетям общего пользования, расположенную в пределах одной контролируемой зоны, без сегментирования, с использованием разных типов операционных систем, многопользовательскую с разграничением прав доступа. Масштаб информационной системы – объектовый, со средним уровнем значимости (УЗ 2) и вторым классом защищенности (К 2) [9].

Для такой системы будут характерны угрозы нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) информации [3]. Актуальными можно признать нижеперечисленные:

– угроза аппаратного сброса пароля bios;

– угроза загрузки нештатной операционной системы;

– угроза использования механизмов авторизации для повышения привилегий;

– угроза неправомерного ознакомления с защищаемой информацией;

– угроза несанкционированного восстановления удалённой защищаемой информации;

– угроза несанкционированного доступа к аутентификационной информации, ее изменение;

– угроза несанкционированного копирования, защищаемой информации, ее модификация, удаление;

– угроза повышения привилегий;

– угроза несанкционированного создания учётной записи пользователя;

– угроза определения топологии вычислительной сети;

– угроза перехвата данных, передаваемых по вычислительной сети;

– угроза подделки записей журнала регистрации событий;

– угроза утраты носителей информации, их форматирование;

– угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

– угроза заражения компьютера при посещении неблагонадёжных сайтов, «фишинга», «фарминга»;

– угроза физического устаревания аппаратных компонентов [5].

Нарушители могут быть как внешними, так и внутренними, иметь потенциал от низкого до высокого уровня.

Политики безопасности обязательно включают в себя следующие позиции: основные принципы обеспечения информационной безопасности, соответствие политики действующему законодательству, ответственность за реализацию политик, ответственность их нарушителей, ликвидация последствий нарушения политики, условия изменения, пересмотра положений политик. Кроме того, в них описаны общие правила обеспечения безопасности информационных техно-

логий при работе сотрудников с ресурсами информационной системы, обязанности ответственного за обеспечение безопасности информации в соответствующем подразделении организации.

Для предотвращения реализации представленных угроз на организационном уровне следует ввести следующие Политики безопасности:

– политика информационной безопасности предприятия;

– политика управления доступом;

– политика управления инцидентами;

– политика использования собственных (мобильных) устройств;

– политика использования паролей;

– политика реализации антивирусной защиты;

– политика уничтожения и утилизации информации на различных носителях;

– политика чистого экрана и рабочего стола;

– политика резервного копирования и восстановления непрерывной работы информационной системы;

– политика передачи информации;

– политика использования ресурсов сети Интернет;

– политика работы с конфиденциальной информацией;

– политика учетных записей.

Разработка нормативно-методических документов на предприятии, таких как политики безопасности всех уровней, различные инструкции, регламенты, положения, правила, позволяет сформулировать и юридически закрепить процессы защиты информации [8].

Внедрение системы управления информационной безопасностью в соответствии с требованиями стандарта ИСО/МЭК 27001, позволит построить управляемый процесс обеспечения ИБ, оптимизировать затраты на ее обеспечение, понизить уровень рисков, связанных с ИБ.

***Список литературы***

1. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: ISO/IEC 27001–2006 от 01.02.2008 г. // Правовой сервер «Консультант Плюс» [Электронный ресурс]. – Режим доступа: www.consultant.ru

2. Вопросы федеральной службы по техническому и экспортному контролю: Указ Президента РФ от 16.08.2004 г. №1085 с изм. и доп. в ред. от 03.02.2015 г. // Официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: fstec.ru

3. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК от 11.02.2013 г. №17 с изм. и доп. в ред. от 01.12.2014 г. // Правовой сервер «Консультант Плюс» [Электронный ресурс]. – Режим доступа: www.consultant.ru

4. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: Приказ ФСТЭК от 14.03.2014 г. №31г. с изм. и доп. в ред. от 17.02.2015 г. // Официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: fstec.ru

5. Банк данных угроз безопасности информации // Официальный сайт банка данных угроз безопасности информации ФСТЭК России» [Электронный ресурс]. – Режим доступа: www.bdu.fstec.ru (дата обращения 26.01.2016).

6. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы: ГОСТ 34.602–89 от 01.01.1990 г. с изм. и доп. в ред. от 16.01.2015 г. / Единая база гостов РФ «ГОСТ эксперт» [Электронный ресурс]. – Режим доступа: www.gostexpert.ru

7. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: ГОСТ Р 51583–2014 от 28.01.2014 г. с изм. и доп. в ред. от 16.01.2015 г. // Библиотека ГОСТов «Все ГОСТы» [Электронный ресурс]. – Режим доступа: vsegost.com

8. Селифанов В.А. Способ моделирования процессов управления техническими средствами и система для его осуществления / В.А. Селифанов, В.В. Селифанов. Патент на изобретение RUS 2331096 08.02.2007.

9. Селифанов В.А. Способ оценки эффективности управления техническими средствами и устройство для его осуществления / В.А. Селифанов, В.В. Селифанов. Патент на изобретение RUS 2338243 16.04.2007.