DOI: 10.17117/na.2015.12.02.029

<http://ucom.ru/doc/na.2015.12.02.029.pdf>

Поступила (Received): 31.12.2015

Белов С.В., Бисалиева А.Х., Ахмедова А.Г., Садыкова У.В. Автоматизированная система поддержки организационных мероприятий по защите информации

**Belov S.V., Bisaliev A.Kh., Akhmedova A.G., Sadykova Yu.V.
Automated support system of organizational measures
of information security**

Предлагаемая к разработке система позволит автоматизировать процессы выполнения организационных мероприятий по обеспечению информационной безопасности и проводить централизованный учет данных мероприятий, необходимых документов, информации по аудитам безопасности

Ключевые слова: информационная безопасность

Offered to the development of the system allows to automate processes for organizational measures of information security and to carry out a central register of these activities, the necessary documents, audit of information security

Key words: information security

Белов Сергей Валерьевич

Кандидат технических наук, доцент, заведующий кафедрой

Астраханский государственный технический университет

г. Астрахань, ул. Татищева, 16

Belov Sergey Valeryevich

Candidate of Engineering Sciences, Associate Professor, Head of Department

Astrakhan state technical university

Astrakhan, Tatischev st., 16

Бисалиева Алия Хаиржановна

Начальник отдела

Астраханский государственный технический университет

г. Астрахань, ул. Татищева, 16

Bisaliev Aliya Khairzhanovna

Head of Department

Astrakhan state technical university

Astrakhan, Tatischev st., 16

Ахмедова Альфия Гайдаровна

Студент

Астраханский государственный технический университет

г. Астрахань, ул. Татищева, 16

Akhmedova Alfiya Gaidarovna

Student

Astrakhan state technical university

Astrakhan, Tatischev st., 16

Садыкова Ульяна Вячеславовна

Студент

Астраханский государственный технический университет

г. Астрахань, ул. Татищева, 16

Sadykova Ulyana Vyacheslavovna

Student

Astrakhan state technical university

Astrakhan, Tatischev st., 16

Существует ряд мер для обеспечения информационной безопасности (далее – ИБ): программно-аппаратные, криптографические, инженерно-технические и

другие меры защиты информации (далее – ЗИ). Однако ключевым элементом в системе защиты информации предприятия являются организационные меры ИБ. Организационные меры предоставляют необходимую административную поддержку техническим решениям, в частности, устанавливают правила эксплуатации информационной системы (далее – ИС) и определяют полномочия и ответственность пользователей. От качества ведения данного рода мероприятий зависит эффективность ЗИ в целом, поскольку организационные мероприятия нацелены посредством выбора конкретных средств и решений реализовать на практике спланированные руководством предприятия меры по ЗИ [2].

Законодательство РФ, а также уполномоченные федеральные органы РФ накладывают ряд требований к организационным мерам по защите конфиденциальной информации, которые прописаны в таких документах: № 152-ФЗ от 27.07.2006 «О персональных данных», постановлении Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказе ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», постановлении Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и др.

К числу таких требований относятся:

- формирование перечня нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС [3];
- классификация ИС и определение уровня защищенности персональных данных при их обработке в ИС;
- определение объектов доступа, предоставление пользователям доступа к объектам;
- формирование модели угроз, включая модель нарушителя;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных [4];
- определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации, и учет машинных носителей конфиденциальной информации;
- регистрация событий безопасности;
- анализ защищенности информации, включая выявление, анализ и устранение уязвимостей в ИС, планирование мероприятий по ИБ, а также ряд иных требований.

Для реализации выполнения требований законодательства РФ целесообразно создать автоматизированную систему (далее – АС), которая позволила бы автоматизировать процессы выполнения организационных мероприятий по обеспечению информационной безопасности и проводить централизованный

учет данных мероприятий, необходимых документов, информации по проводимым аудитам безопасности и пр. Схема АС представлена на рисунке 1.

Входными данными для АС являются информация об инфраструктуре организации (список сотрудников, должностей, отделов, ответственных лиц), загружаемая из ПО «1С: Предприятие» (данный продукт выбран исходя из масштабности его использования в РФ), информация об особенностях организации и сфере ее деятельности, базы знаний по требованиям уполномоченных органов, законодательства РФ и рекомендаций государственных стандартов. Конечным результатом являются документы и отчетности в соответствии с требованиями законодательства РФ. Кроме того, АС должна обеспечивать выгрузку данных по примененным правилам безопасности в «1С: Зарплата и управление персоналом» для реализации материального стимулирования сотрудников организации.

Рис. 1. Структура АС поддержки организационных мероприятий по ЗИ

Разработку модели угроз планируется реализовать отдельным модулем, на основе проекта документа «Методика определения угроз безопасности информации в информационных системах», опубликованного ФСТЭК России 7 мая 2015 г. Методика предназначена для государственных информационных систем, защита информации в которых обеспечивается в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Методика может применяться как на этапах создания информационных систем, так и в ходе их эксплуатации при периодическом пересмотре (переоценке) угроз безопасности информации.

Методика определения угроз предполагает реализацию непрерывного процесса, в рамках которого определяется область применения процесса опре-

деления угроз, идентифицируются источники угроз и угрозы безопасности информации, оценивается возможность реализации угроз безопасности информации и степень возможного ущерба в случае такой реализации, осуществляется мониторинг и переоценка угроз безопасности информации.

При идентификации источников угроз необходимо оценить следующие параметры:

- типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;
- возможные способы реализации угроз безопасности информации.

Актуальность угрозы безопасности информации определяется на основе следующих данных:

- статистические данные о частоте реализации угроз безопасности информации;
- уровень защищенности (проектной) информационной системы;
- потенциал нарушителя;
- степень возможного ущерба в случае реализации угрозы.

В качестве исходных данных об угрозах безопасности информации и их характеристиках используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России [1], а также базовые и типовые модели угроз безопасности информации, разрабатываемые ФСТЭК России для различных классов и типов информационных систем. На основе данной методики определения угроз безопасности информации разрабатывается информационная система оценки угроз на предприятии, являющаяся подсистемой АС поддержки организационных мероприятий по защите информации. Структура ИС оценки угроз представлена на рисунке 2.

Рис. 2. Структура ИС оценки угроз на предприятии

Таким образом, автоматизированная система поддержки организационных мероприятий, включающая модуль построения модели угроз, поможет решить задачи, связанные с выполнением специалистами требований по информационной безопасности, контролем по соответствию требованиям законодательства РФ, а также поможет сократить временные затраты на создание документации по информационной безопасности и проведение аудитов.

Список используемых источников:

1. Банк данных угроз безопасности информации URL: <http://bdu.fstec.ru>
2. Организационные основы защиты информации на предприятии.
URL: <http://bezopasnik.org/article/19.htm>
3. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
4. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

© 2015, Белов С.В., Бисалиева А.Х., Ахмедова А.Г.,
Садыкова У.В.

*Автоматизированная система поддержки
организационных мероприятий по защите
информации*

© 2015, Belov S.V., Bisaliev A.Kh., Akhmedova A.G.,
Sadykova Yu.V.

*Automated support system of organizational
measures of information security*