МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ООО «ВЕКТОР-К»

Сборник тезисов докладов Консультационно-экспертного мероприятия «Повышение информационной безопасности в сфере научной и инновационной деятельности»

Москва
2016

УДК 351

Сборник тезисов докладов Консультационно-экспертного мероприятия «**Повышение информационной безопасности в сфере научной и инновационной деятельности**», Выпуск 6. – М.: «ВЕКТОР – К», 2016. -7 стр.

В издании «Сборник тезисов докладов консультационно-экспертного мероприятия «**Повышение информационной безопасности в сфере научной и инновационной деятельности**», представлены тезисы докладов мероприятия с участием представителей вузовского сектора исследований и разработок, направленного на развитие взаимодействия и повышение эффективности управления в сфере научной и инновационной деятельностью, проведенного 23 сентября 2016 года в Москве.

ООО «ВЕКТОР-К»
УДК 351

Консультационно-экспертное мероприятие
«Повышение информационной безопасности в сфере научной и инновационной деятельности»

1. **«Основополагающие нормативные документы и требования к защите информации»»**

Юсубалиев Т.Р., ООО «Качественные Программные Решения»

В настоящее время в сфере научной и инновационной деятельности существует проблема информационной безопасности. Важным является не только детальное описание технологии, но и проблема сохранения авторства и патентообладания.

Защита информации, как обобщенный термин, подразумевающий под собой хранение и передачу информации без рисков раскрытия данной информации третьим лицам, играют важную роль в процессе деятельности компаний и государственных организаций.

В настоящее время, основными организационно-распорядительными документами в области защиты информации являются:

- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (действующая редакция, 2016)

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

ФСТЭК России является федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически

важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения её утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Организационно-административное обеспечение безопасности информации представляет собой регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, чтобы разглашение, утечка и несанкционированный доступ к информации становился невозможным или существенно затруднялся за счет проведения организационных мероприятий. К мерам этого класса можно отнести: подбор и обучение персонала, определение должностных инструкций работников, организацию пропускного режима, охрану помещений, организацию защиты информации с проведением контроля работы персонала с информацией, определение порядка хранения, резервирования, уничтожения конфиденциальной информации и т.п.

2. «Обеспечение организационной безопасности информационных систем»

Бобов П.К., ООО «Качественные Программные Решения»

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе — раскрывает ее структуру на уровне объективизации. Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств. Основные направления организационной защиты информации приведены ниже.

Организационная защита информации:

- Организация работы с персоналом;
- Организация внутреннего и пропускного режимов и охраны;
- Организация работы с носителями сведений;
- Комплексное планирование мероприятий по защите информации;
- Организация аналитической работы и контроля.

Основные принципы организационной защиты информации:

- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

Компания Качественные программные решения специализируется на оказании услуг по разработке, обеспечению качества и безопасности программного обеспечения для коммерческих и государственных организаций.

ООО “КПР” был выявлен оптимальный порядок организации мероприятий по защите информации, который носит рекомендательный характер:

1. Формирование требований к защите информации, содержащейся в информационной системе.
2. Разработка системы защиты информации информационной системы.
3. Внедрение системы защиты информации информационной системы.
4. Аттестация информационной системы по требованиям защиты информации и ввод ее в действие.
5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.
6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

На этапе формирования требований к защите информации руководствуются ГОСТами 51583 и 51624.

3. «Обеспечение технической защиты данных в информационных системах»

Дорофеев Д.И., ООО «Качественные Программные Решения»

Инженерно-технические меры представляют собой совокупность специальных органов, технических средств и мероприятий, функционирующих совместно для

выполнения определенной задачи по защите информации. К инженерным средствам относят экранирование помещений, организация сигнализации, охрана помещений с ПК.

Технические средства защиты включают в себя аппаратные, программные, криптографические средства защиты, которые затрудняют возможность атаки, помогают обнаружить факт ее возникновения, избавиться от последствий атаки.

Технические средства подсистем безопасности современных распределенных информационных систем выполняют следующие основные функции:

– аутентификация партнеров по взаимодействию, позволяющая убедиться в подлинности партнера при установлении соединения;

– аутентификация источника информации, позволяющая убедиться в подлинности источника сообщения;

– управление доступом, обеспечивающее защиту от несанкционированного использования ресурсов;

– конфиденциальность данных, которая обеспечивает защиту от несанкционированного получения информации;

– целостность данных, позволяющая обнаружить, а в некоторых случаях и предотвратить изменение информации при ее хранении и передаче;

– принадлежность, которая обеспечивает доказательство принадлежности информации определенному лицу.

Для реализации указанных функций используются следующие механизмы:

– шифрование, преобразующее информацию в форму, недоступную для понимания неавторизованными пользователями (подробнее шифрование рассматривается в главе 2);

– электронная цифровая подпись, переносящая свойства реальной подписи на электронные документы (подробнее см. гл.4);

– механизмы управления доступом, которые управляют процессом доступа к ресурсам пользователей на основе такой информации как базы данных управления доступом, пароли, метки безопасности, время доступа, маршрут доступа, длительность доступа;

– механизмы контроля целостности, контролирующие целостность как отдельного сообщения, так и потока сообщений и использующие для этого контрольные суммы, специальные метки, порядковые номера сообщений, криптографические методы;

– механизмы аутентификации, которые на основании предъявляемых пользователем паролей, аутентифицирующих устройств или его биометрических параметров принимают решение о том, является ли пользователь тем, за кого себя выдает (подробнее см. гл.3);

– механизмы дополнения трафика, добавляющие в поток сообщений дополнительную информацию, «маскирующую» от злоумышленника полезную информацию;

– механизмы нотаризации, которые служат для заверения подлинности источника информации.

ООО «ВЕКТОР-К»
Москва 2016