Аналитические материалы по результатам

Консультационно-экспертное мероприятие «Повышение информационной безопасности в сфере научной и инновационной деятельности» от 23 сентября 2016 года

Место проведения: Новотель Москва Центр, конференц-зал “Мадрид”

Адрес проведения: г. Москва, ул. Новослободская, д. 23

Дата проведения: 23 сентября 2016 года

Заказчик: Министерство образования и науки Российской Федерации

Организаторы: ООО «ВЕКТОР-К»

Участники:	Представители образовательных организаций высшего образования, Представители сектора исследований и разработок, Представители – эксперты.

Цель: ознакомление студентов, аспирантов и молодых специалистов с проблематикой информационной безопасности, сохранения авторства и патентообладания, с основными информационными системами и анализом уязвимостей.

Задача мероприятия: повышение информированности участников процесса о проблемах взлома информационных систем и существующих методах их решения;

повышение информированности участников процесса об исследовании систем на наличие уязвимостей;

повышение информированности участников процесса об аудите систем на соответствие требованиям законодательства и международным стандартам;

Регламент мероприятия

Время	Тема доклада/ФИО, должность докладчика
11.00-11.30	**Регистрация, тестирование связи**
11.00-11.30	**Кофе-брейк**
11.30-11.40	**Вступительное слово модератора мероприятия** *Табаков К.В., ООО «ВЕКТОР-К»*
11.40-12.00	**«Основополагающие нормативные документы и требования к защите информации»** *Юсубалиев Т.Р., ООО «Качественные Программные Решения»*
12.00-12.10	**Обсуждение доклада, вопросы к докладчику**
12.10-12.30	**«Обеспечение организационной безопасности информационных систем»** *Бобов П.К. ООО «Качественные Программные Решения»*
12.30-12.40	**Обсуждение доклада, вопросы к докладчику**
12.40-13.10	**Кофе-брейк**
13.10-13.30	**«Обеспечение технической защиты данных в информационных системах»** *Дорофеев Д.И., ООО «Качественные Программные Решения»*
13.30-14.10	**Обсуждение доклада, вопросы к докладчику, дискуссия**
14.10-14.20	**Подведение итогов совещания, заключительное слово** *Табаков К.В., ООО «ВЕКТОР-К»*

Результаты проведенных обсуждений

В результате обсуждений были получены рекомендации по минимальным требованиям безопасности систем. В системах должны строго выдерживаться сложность и регулярность смены паролей, обмен информацией и доступ к системе - исключительно через безопасные и защищенные каналы связи, не должны быть использованы лишние порты. Была затронута проблематика небрежности в отношении сохранности конфиденциальных данных авторизации и пути ее ликвидации.

Тезисы доклада: «Основополагающие нормативные документы и требования к защите информации»

Юсубалиев Т.Р.:

В настоящее время в сфере научной и инновационной деятельности существует проблема информационной безопасности.

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.

Тезисы доклада: «Обеспечение организационной безопасности информационных систем»

Бобов П.К.:

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 в компании — регламентация деятельности и взаимоотношений субъектов (сотрудников компании) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данной компании.

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:

- 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.

В качестве основного принципа организационной защиты информации следует выделить 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.

Тезисы доклада: «Обеспечение технической защиты данных в информационных системах».

Дорофеев Д.И.:

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

– электронная цифровая подпись, переносящая свойства реальной подписи на электронные документы;

– 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;

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

механизмы нотаризации, которые служат для заверения подлинности источника информации.

Выводы и предложения:

В настоящее время научный потенциал определяется уровнем развития информационной инфраструктуры. Как следствие, пропорционально увеличивается потенциальная уязвимость научных исследований по отношению к информационным воздействиям.

С позиций системного подхода к защите информации необходимо использовать средства защиты во всех структурных элементах и на всех этапах цикла обработки информации. Методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа информации. Планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации. Необходима четкость в осуществлении полномочий и прав пользователей на доступ к определенным видам информации, в обеспечении контроля средств защиты и немедленного реагирования на их выход из строя.

Сегодня обобщенная теория безопасности информации пока не создана. Применяемые на практике подходы и средства нередко страдают существенными недостатками и не обладают объявленной надежностью. Поэтому необходимо обладать достаточной подготовкой и квалифицированно ориентироваться во всем спектре вопросов обеспечения информационной безопасности, понимая их комплексный и взаимообусловленный характер.

Ввиду быстрой динамики развития технологий и Интернета защита информации является одним из наиболее приоритетных направлений не только в области научной и исследовательской деятельности, но и в любой развивающейся отрасли в целом.

По статистике, госучреждения – не самый сложный соперник для кибермошенников и хакеров, как из-за низкого качества выполнения услуг безопасности подрядчиком, так и человеческий фактор из-за слабой организации мероприятий по защите информационной безопасности.

Предлагается реорганизация логики работы комиссий и экспертных групп, курирующих деятельность организаций по мероприятиям информационной безопасности с целью повышения эффективности обнаружения и устранения оказываемых неквалифицированных услуг в данной сфере. Введение дополнительных мероприятий и организационных собраний по данной тематике поможет минимизировать риск утечки информации вследствие повышения информированности персонала в данной области. Также регулярное проведение мероприятий снижает риск ошибки из-за “человеческого фактора”.

Приложение 1

Список участников

1	Белениккин Максим Сергеевич	Московский физико-технический институт (государственный университет)
2	Кантимирова Элина Юнировна	Московский физико-технический институт (государственный университет)
3	Мельникова Наталия Владимировна	ИМБ РАН
4	Новиков Юрий Александрович	Московский физико-технический институт (государственный университет)
5	Обухан Вячеслав Геннадиевич	ЗАО "Московский центр трансфера технологий"
6	Чермянин Георгий Константинович	Московский физико-технический институт (государственный университет)
7	Юсубалиев Тимур Ринатович	ООО «Качественные Программные Решения»
8	Бобов Петр Кириллович	ООО «Качественные Программные Решения»
9	Дорофеев Дмитрий Иванович	ООО «Качественные Программные Решения»
10	Табаков Кирилл Викторович	ООО «ВЕКТОР-К»
11	Александров Андрей Вячеславович	ООО «ВЕКТОР-К»