НОВИКОМБАНК

Актуальные вопросы информационной безопасности предприятий оборонно-промышленного комплекса Российской Федерации

Руководитель Службы информационной безопасности

Макоско А.А.

НОВИКОМБАНК

Ежегодно в России увеличивается количество киберпреступлений, атаки на предприятия и их клиентов совершаются постоянно. Активизировались преступные группы, которые способны проникнуть в сеть предприятия, добраться до изолированных систем.

Для противостояния современным угрозам информационной безопасности и снижению их влияния на деятельность предприятия, необходимо обеспечить необходимый и достаточный уровень защиты информации.

НОВИКОМБАНК

Цели развития системы обеспечения информационной безопасности

1. Техническая защита от угроз информационной безопасности всех информационных систем.
2. Обеспечение соответствия информационных систем требованиям законодательства РФ в области информационной безопасности.
3. Улучшение совместно с другими структурными подразделениями процессов управления доступом работников к информационным системам.
4. Создание и актуализация существующих внутренних нормативных документов по информационной безопасности.
5. Обеспечение качественного, эффективного и регулярного повышения осведомленности работников в области информационной безопасности.
6. Мониторинг выполнения требований внутренних нормативных документов по информационной безопасности всеми работниками предприятия.
7. Оптимизация управления криптографическими средствами в системах.

НОВИКОМБАНК

Основные источники угроз

- уязвимости в информационных системах, в том числе использование устаревших версий программного обеспечения;
- выполнение вредоносных программ;
- использование нелицензионного программного обеспечения;
- ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла;
- нарушение функциональности криптографической системы;
- компрометация удаленного доступа;
- сбои и отказы программного обеспечения, технических средств и каналов связи;
- нарушение электропитания оборудования, на котором работают информационные системы;

НОВИКОМБАНК

Основные источники угроз

- социальная инженерия;
- зависимость от партнеров/ клиентов, реализующих бизнес процессы, содержащие уязвимые приложения и сервисы;
- невысокие компетенции в области безопасной разработки программного обеспечения у вендоров ПО;
- ошибки, допущенные при заключении договоров;
- нарушение договорных обязательств третьими лицами;
- использование некачественной нормативной документации, в том числе несоответствующей законодательству;
- нарушение работниками утвержденных на предприятии требований по обеспечению информационной безопасности (недобросовестное исполнение обязанностей, халатность, ошибки, хищения информации и т.д.);
- действия внешних нарушителей.

НОВИКОМБАНК

В целях нейтрализации источников угроз и снижения рисков информационной безопасности, необходимо руководствоваться лучшими практиками – Стандартами в области информационной безопасности и в соответствии с которыми «строить» ИБ на предприятии. Одним из самых популярных сегодня является международный стандарт серии ISO/IEC 27XXX.

Также следует учитывать технический Стандарт обеспечения ИБ ГК РОСТЕХ, который описывает технические мероприятия по защите информации для 11 основных подсистем.

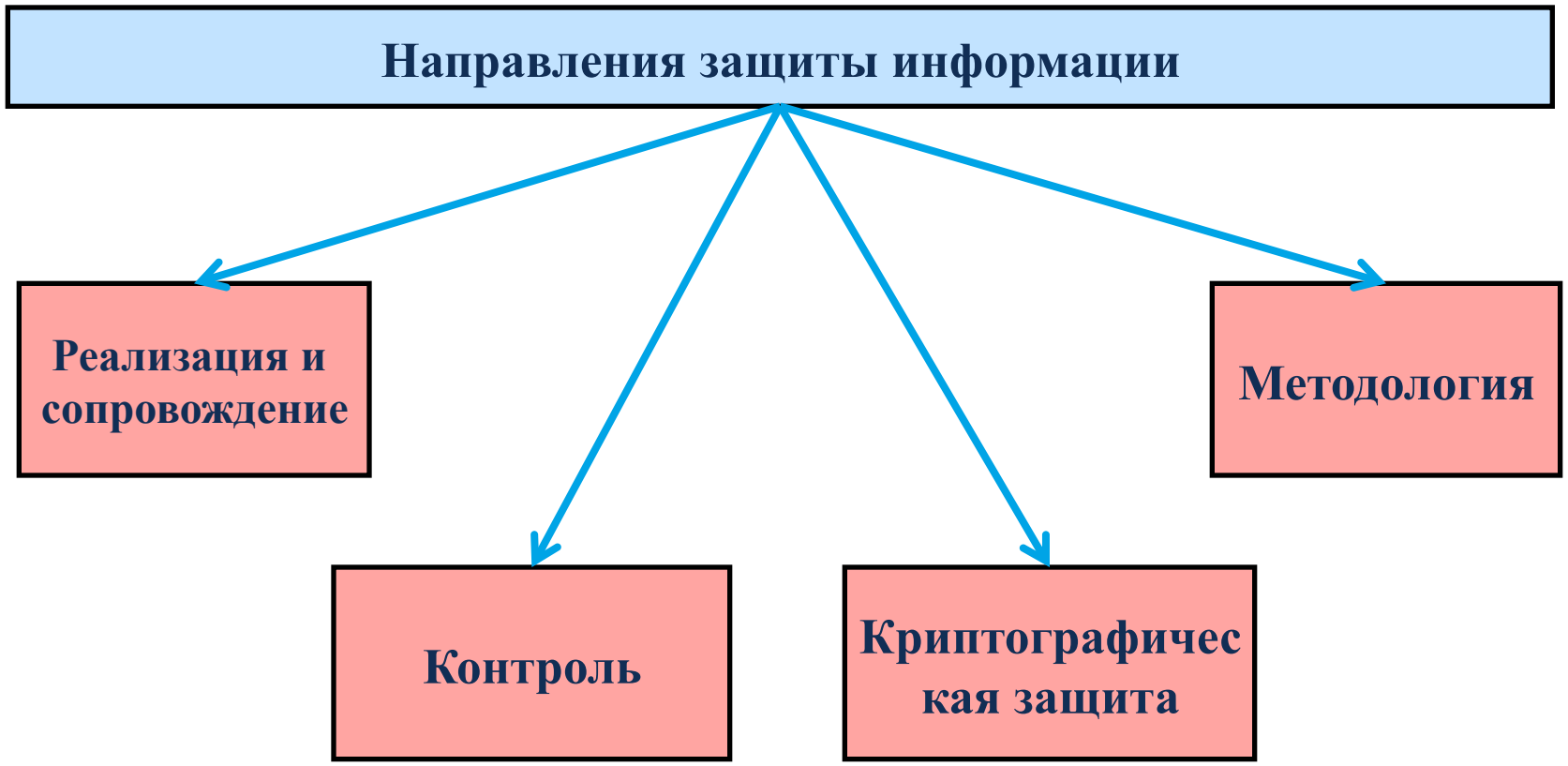
Далее необходимы ресурсы, в частности создать подразделение информационной безопасности, разработать и утвердить руководством предприятия Стратегию обеспечения информационной безопасности на 3-5 лет вперед, в которой указать организационные и технические мероприятия.

НОВИКОМБАНК

Для реализации и поддержания ИБ на предприятии необходима реализация четырех групп процессов:

НОВИКОМБАНК

РАБОТЫ СЛЕДУЕТ ПЛАНИРОВАТЬ ПО ЧЕТЫРЕМ ОСНОВНЫМ НАПРАВЛЕНИЯМ ЗАЩИТЫ ИНФОРМАЦИИ



НОВИКОМБАНК

Технические мероприятия

- система эшелонированной защиты от вредоносного кода на различных уровнях информационной инфраструктуры;
- система межсетевого экранирования;
- криптографическая система защиты информации;
- система защиты от НСД, в том числе парольная;
- система доступа в информационно-телекоммуникационную сеть Интернет, включающая в себя как централизованную технологию терминального доступа для всех работников, так и внедрение специализированного программно-аппаратного комплекса, позволяющего категорировать используемые ресурсы, разграничивать полномочия, а также проводить онлайн проверку получаемой из сети Интернет информации и очистку ее от вредоносного программного обеспечения, защищая от действий злоумышленников (в том числе противодействуя методам социальной инженерии);

НОВИКОМБАНК

Технические мероприятия

- система предотвращения утечек конфиденциальной информации (DLP), контролирующей и/или закрывающей все используемые каналы обмена информацией с внешними информационными системами с закрытием доступа к портам (USB, DVD, CD, дисковод и т.д), за исключением тех, кому порты необходимы для выполнения должностных обязанностей;

- система защиты от DDoS – атак, в том числе с привлечением провайдеров услуг и/или отдельных CPE решений;

- системы защиты web и почтового трафика, в том числе, специально выделенной среды для безопасного исполнения компьютерных программ и системы обнаружения целевых атак, а также защиты от СПАМа;

- система контроля, управления и защиты обрабатываемой информации для удаленных рабочих мест (в том числе мобильных) с использованием удаленного доступа или с организацией защиты хранимых на удаленном устройстве данных (MDM, капсулирование и т.д.);

- система защиты средств виртуализации;

НОВИКОМБАНК

Технические мероприятия

- система защиты, направленная на обеспечение безопасности критичных веб-сервисов и приложений (WAF);
- центр мониторинга SOC свой или использование SOC ГК РОСТЕХ – система выявления и обработки инцидентов;
- система сбора, анализа и корреляции событий ИБ (SIEM);
- система обнаружения и предотвращения сетевых вторжений (IDS/IPS);
- система контроля сетевых конфигураций;
- система управления правами доступа (IDM);
- автоматизированные сканеры программного кода, позволяющих эффективно и достоверно организовать процесс поиска и устранения уязвимостей в программных комплексах на этапе их разработки, либо доработки отдельных модулей;
- система регистрации и контроля всех действий пользователей, обладающих привилегированными полномочиями (администраторов информационных систем, представителей компаний-разработчиков и т.п.).

НОВИКОМБАНК

Организационные мероприятия

- проведение на регулярной основе аудитов (с привлечение работников сторонней организации) и самооценок соответствия ИБ требованиям Стандарта;
- проведение оценки рисков нарушения ИБ в рамках построения/ совершенствования системы обеспечения ИБ в соответствии с требованиями нормативных документов;
- постоянное взаимодействие с регуляторами по противодействию кибератакам;
- повышение осведомленности работников в области информационной безопасности;
- обеспечение централизованного подхода в архитектуре построения системы менеджмента информационной безопасности;

НОВИКОМБАНК

Организационные мероприятия

- ежегодная организация проведения тестирования (с привлечением работников сторонней организации) на возможность проникновения внешнего нарушителя ИБ в информационные системы и внутренний анализ защищенности систем (внутренний нарушитель ИБ);

- создание и постоянное обновление нормативной базы предприятия в области ИБ.

Для развития и совершенствования системы обеспечения информационной безопасности критически важным является вовлечение работников ИБ во все проекты по разработке, развитию и совершенствованию, как информационных систем, так и бизнес-процессов.

НОВИКОМБАНК

В целях повышения уровня информационной безопасности необходимо постоянно проводить работы по построению комплексной и эшелонированной системы защиты, в соответствии с требованиями законодательства Российской Федерации, нормативных актов регулирующих и надзорных органов, а также нормативных документов предприятия в области информационной безопасности.

НОВИКОМБАНК

Спасибо за внимание!