Головинский Анатолий Александрович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Синяков Евгений Анатольевич
Преподаватель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Чухров Роман Вячеславович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

Кузнецов Илья Олегович
Слушатель, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко
Краснодар

АЛГОРИТМ ДЕЯТЕЛЬНОСТИ РУКОВОДИТЕЛЯ ПОДРАЗДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИЗМЕНЕНИИ ОРГАНИЗАЦИОННО ШТАТНОЙ СТРУКТУРЫ ПРЕДПРИЯТИЯ

Аннотация: в статье рассматриваются этапы и особенности работы руководителя подразделения информационной безопасности (ИБ) в условиях изменения организационно-штатной структуры (ОШС) предприятия.

Ключевые слова: информационная безопасность, организационная структура, риски, нормативные документы, управление изменениями, защита информации.

1. Анализ предстоящих изменений

Первый этап алгоритма — получение и анализ информации о предстоящих изменениях в ОШС. Руководитель ИБ должен:

- Запросить проект новой ОШС;
- Оценить потенциальное влияние на систему ИБ;
- Выявить зоны риска: изменение ролей, увольнение ключевых сотрудников, объединение/ликвидация подразделений.

2. Участие в межфункциональных коммуникациях

Необходимо включиться в рабочие группы по реструктуризации для:

- Защиты интересов ИБ;
- Координации с HR, юридическим отделом, ИТ-подразделением;
- Обеспечения учета требований ИБ при изменении бизнес-процессов.

3.Обновление нормативной базы ИБ

После утверждения изменений руководитель ИБ инициирует пересмотр следующих документов:

- Политики и регламенты доступа к информации;
- Положения о подразделении ИБ;
- Модель угроз и рисков;
- Регламент реагирования на инциденты.

4. Актуализация модели доступа и прав

Изменения в ОШС требуют пересмотра:

- Ролевой модели доступа;
- Матрицы разграничения прав;
- Привилегий пользователей, в том числе административных.

Важно предотвратить как несанкционированный доступ, так и простои, вызванные потерей доступа.

5. Проведение оценки новых рисков

Следующий шаг — повторная оценка рисков с учетом новых условий:

- Перемещение конфиденциальной информации между подразделениями;
- Увольнение сотрудников с доступом к критическим системам;
- Появление новых каналов утечки информации.

6. Обучение и информирование персонала

Руководитель подразделения ИБ организует:

Обновление программ по ИБ с учетом новых реалий;

Проведение инструктажей и рассылок;

Повышение осведомленности новых сотрудников и руководителей.

7. Мониторинг и контроль

После внедрения изменений осуществляется усиленный контроль:

- Мониторинг событий ИБ в новых зонах риска;
- Оценка эффективности новых мер защиты;
- Подготовка отчетности для высшего руководства.

Данный алгоритм можно представить в виде блок-схемы

Заключение

Изменение ОШС — критический момент, требующий активных и системных действий от руководителя подразделения ИБ. Четкий алгоритм действий позволяет не только снизить риски, но и повысить зрелость системы информационной безопасности в новых условиях.

Список литературы:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2022681284 Российская Федерация. Программа по учету средств криптографической защиты информации : № 2022680691 : заявл. 24.10.2022 : опубл. 11.11.2022 / А. В. Акишин, Н. Н. Енин, С. Н. Ершов [и др.]. – EDN QIXXPV.

2. Свидетельство о государственной регистрации базы данных № 2019621548 Российская Федерация. Информационная система по учету и обработке данных для подразделений защиты информации ("Akishin_LS 8.0") : № 2019621403 : заявл. 15.08.2019 : опубл. 02.09.2019 / А. А. Бречко, Р. Д. Фатьянов, И. А. Федяева [и др.]. – EDN YTQUXF.

3. Свидетельство о государственной регистрации программы для ЭВМ № 2024618327 Российская Федерация. Информационно-справочная система учета движения МНИ в организациях : № 2024617042 : заявл. 01.04.2024 : опубл. 10.04.2024 / Е. В. Якель, Д. П. Нечаев, М. С. Бодякин [и др.] ; заявитель Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации. – EDN SOGRCQ.

4. Анализ проблем применения программного обеспечениядля создания систем поддержки принятия решений должностных лиц подразделений информационной безопасности / Д. А. Охотин, А. В. Акишин, Е. С. Уколов [и др.] // Вектор научной мысли. – 2025. – № 1(18). – С. 323-325. – EDN EFSNBN.

5. Свидетельство о государственной регистрации программы для ЭВМ № 2023669474 Российская Федерация. Программа поддержки принятия решений руководителя подразделения информационной безопасности : № 2023668535 : заявл. 30.08.2023 : опубл. 14.09.2023 / А. В. Акишин, Д. А. Ржевский, Р. В. Лукьянов [и др.]. – EDN DHOEBO.