ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А. А. Бабенко

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

(Волгоградский государственный университет)

Управление рисками информационной безопасности (ИБ) в государственных информационных системах (ГИС) актуально в связи с: возрастанием числа угроз, обусловленными экономическими и политическими событиями в мире; необходимостью выполнения требований законодательства о защите ГИС; ценностью информации, обрабатываемой в ГИС для злоумышленников; ростом роли ГИС в цифровизации экономики РФ.

Анализ ГИС, зарегистрированных в Реестре Федеральных ГИС, показал, что в них обрабатывается конфиденциальная информация, ПДн, а также др. виды информации. Требования к определению класса защищенности ГИС сформулированы в 17 приказе ФСТЭК. Классификацию ГИС производит оператор, если на базе ГИС функционирует сервер государственного или муниципального органа.

По степени конфиденциальности информацию, обрабатываемую в ГИС, делят на: особой важности (ОВ), совершенно секретную (СС), секретную (С), конфиденциальную.

На состав системы защиты информации ГИС, оказывают влияние такие факторы, как: обработка разных видов информационных ресурсов с различной ценностью; распределенность узлов, в составе ГИС; необходимость соблюдения требований нормативно-правовых актов на всех этапах жизненного цикла ГИС; сложный состав программно-аппаратных платформ, обеспечивающих работу ГИС и средств их защиты; подключение к системам общего пользования; разделение потока информации в ГИС на внешний и внутренний.

Жизненный цикл ГИС регламентируется требованиями [1], согласно которым ИБ ГИС, технические задания на создание ГИС согласуются с ФСТЭК.

Согласно статистике Infowatch за 2017-2021 г.г. больше всего атак совершается на АРМ ГИС – 35,5%: эксплуатация уязвимостей, вредоносное ПО, подбор паролей и нарушение политик ИБ. Отмечается что внутренний нарушитель наиболее частая причина утечек информации – 64,5%. Чаще всего злоумышленников интересуют ПДн и платежная информация, а каналы их утечки – сеть и бумажные документы [2].

Для формирования актуального перечня угроз ИБ ГИС применяется БДУ безопасности информации ФСТЭК и международные БД и другие источники об уязвимостях и угрозах ИБ.

Для управления рисками информационной безопасности в государственных информационных системах мы предлагаем программный комплекс, основными функциями которого являются:

1) экспертная идентификация ценных активов, угроз и мер защиты ГИС [3];
2) построение экспертом связей между активами, угрозами и техническими мерами защиты;
3) количественная и качественная оценка экспертом ценности активов ГИС;
4) экспертная оценка частного риска ИБ для каждой угрозы активам ГИС [4];
5) определение уровня рассчитанных рисков ИБ активов ГИС;
6) определение экспертом технических мер защиты активов ГИС от угроз ИБ;
7) формирование отчетов о составе системы защиты активов ГИС и остаточном риске после их обработки [5].

Архитектура системы управления рисками информационной безопасности в ГИС представлена на рисунке 1.

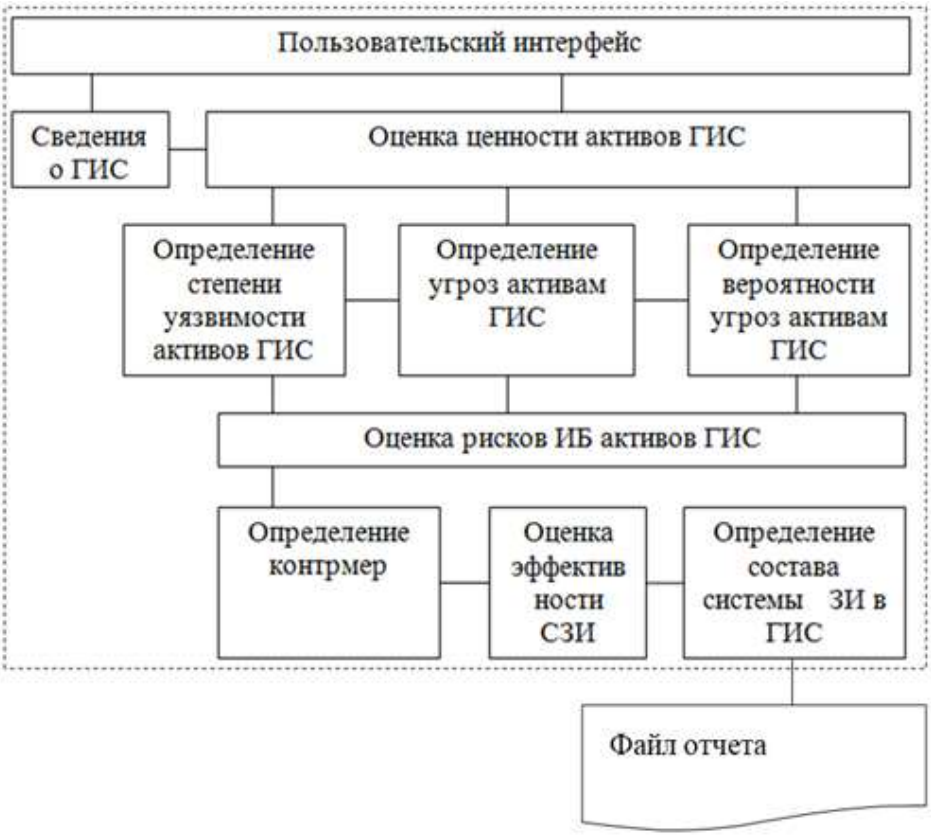

Рис. 1. Архитектура системы управления рисками информационной безопасности в ГИС

Входными данными для системы управления рисками информационной безопасности в государственных информационных системах, будут – активы ГИС и их ценность, список угроз активам ГИС и их вероятность, степень уязвимости активов ГИС актуальным угрозам, список мер и средств защиты, значения критериев для их сравнения.

Выходными данными – значения риска для угроз активам ГИС, состав системы защиты информации в ГИС, значения остаточного риска для угроз активам ГИС.

Описание модулей системы управления рисками информационной безопасности в государственных информационных системах представлено в таблице 1.

Таблица 1. Модули системы управления рисками информационной безопасности в ГИС

Обозначение модуля	**Задачи, решаемые модулем**
Пользовательский интерфейс	Состоит из вкладок для ввода экспертом данных и вывод результатов работы.
Сведения о ГИС	Сбор сведений о ГИС, её активах, их классификация
Оценка ценности активов ГИС	Определение активов ГИС и их ценности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010.
Определение угроз активам ГИС	Определение угроз ИБ ценным активам ГИС, в соответствии с БДУ ФСТЭК и др. источников.
Определение степени уязвимости активов ГИС	Представляет результат экспертной оценки уязвимости актива ГИС для ранее установленного перечня угроз, по количественной шкале
Определение вероятности угроз активам ГИС	Представляет результат экспертной оценки вероятности реализации угроз ИБ активам ГИС
Оценка рисков ИБ активов ГИС	Представляет отчет об оценке рисков ИБ для каждого из ценных активов ГИС
Определение контрмер	Для экспертного принятия решения о выборе защиты активов ГИС, риски которых признаны неприемлемыми и подлежат обработке с целью их минимизации.
Оценка эффективности СЗИ	Для экспертного выбора наиболее рациональных СЗИ в ГИС в соответствии с критериями [2].
Определение состава системы ТЗИ в ГИС	Отчет о составе системы ЗИ в ГИС после обработки рисков ИБ активов ГИС и остаточном риске для каждой из актуальных угроз после их обработки.
Файл отчета	Файл в формате *.xlsx для хранения и последующего использования информации обрабатываемой в системе управления.

Предложенная архитектура позволяет разработать систему управления рисками информационной безопасности в ГИС, которая поможет эксперту провести оценку рисков ИБ для активов ГИС и минимизировать последствия от них, определив контрмеры и состав системы защиты информации, минимизирующий вероятность реализации существующих угроз ИБ.

Литература

1. Жуйкова С.А., Курина А.Д., Бабенко А.А. Модель оценки рисков на различных этапах жизненного цикла информационной системы. – Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике. материалы VII Всероссийской научно-практической конференции. Волгоградский государственный университет. 2018. С. 233-238.

2. Бабенко А.А., Козунова С.С. Модель определения состава системы защиты информации в государственной информационной системе. – Информационные системы и технологии. 2021. № 2 (124). С. 92-101.

3. Бабенко А.А. Экспертный метод определения состава системы технической защиты информации в государственных информационных системах. – Перспективные информационные технологии (ПИТ 2021). Труды Международной научно-технической конференции. под ред. С.А. Прохорова. Самара, 2021. С. 136-139.

4. Бабенко А.А., Магомедов Д.А. Оценка риска информационной безопасности автоматизированной системы управления технологическим процессом. – Перспективные информационные технологии (ПИТ 2021). Труды Международной научно-технической конференции. под ред. С.А. Прохорова. Самара, 2021. С. 140-145.

5. Бабенко А.А. Жарков Г.В. Программа определение состава системы технической защиты информации в государственных системах: св-во о гос. рег. прогр. для ЭВМ 2020615502 Российская Федерация. Зарегист. 25.05.2020.

А.А. Бабенко, А.А. Вдовкин

АЛГОРИТМ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НЕФТЕГАЗОВОЙ ОТРАСЛИ

(Волгоградский государственный университет)

Защита объектов нефтехимического и нефтегазового производства является актуальной проблемой. Остро стоит необходимость решения технических и программных вопросов безопасности технологических процессов. Современные бизнес системы во многом базируются на информационной сфере, что требует поддержания определенного уровня информационной безопасности включающей в себя программно-аппаратные, технические и организационные меры защиты на всех уровнях управления [1, 2].