Ответ к заданию. Моделирование угроз

Вопрос 1.

Напишите возможные негативные последствия от реализации (возникновения) угроз безопасности информации. 3 самых негативных для выбранного актива. Напишите, почему выбрали их.

Актив предприятия для которого разрабатывается модель угроз:
Программный код прошивки BIOS (КТ).
Организация занимается разработкой средств защиты информации и занимает лидирующее место на мировом рынке.

!!!В работе используйте Приложение 4 из Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.

№	Виды риска	Негативные последствия	Обоснование
1	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Прошивка BIOS – ключевой актив компании, ее утечка приведет к потере конкурентного преимущества; Злоумышленники могут копировать или модифицировать код, что может повлечь выпуск пиратских версий, снижение рыночной стоимости продукта, утрату доверия клиентов.
2	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов.	Компания работает на мировом рынке, где соблюдение стандартов (например, ФСТЭК) критично. Утечка или компрометация BIOS может привести, например, к аннулированию сертификатов, потере допусков к госзаказам, санкциям по международным контрактам.
3	Ущерб физическому лицу	Нарушение конфиденциальности	Если злоумышленник воспользуется

		(утечка) персональных данных.	уязвимостью в BIOS, он может, например, получить доступ к паролям, банковским данным, личным файлам. Внедрить вредоносный код (например, кейлоггеры, бэкдоры). Последствиями могут быть кража денег, шантаж, мошенничество.

Вопрос 2.

Какие есть возможные объекты воздействия угроз безопасности информации? Напишите не менее 3-х.

!!!В работе используйте Приложение 5 из Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.

№	Возможные объекты воздействия угроз безопасности
1	Система управления и администрирования
2	Автоматизированное рабочее место пользователя
3	Системы хранения данных (базы данных, СУБД)

Вопрос 3.

Опишите возможные способы реализации (возникновения) угроз безопасности информации. Напишите не менее 5-ти.

!!!В работе используйте Приложение 10 из Методики оценки угроз безопасности от ФСТЭК России от 05 февраля 2021 г.

Если в кейсе речь идет о компрометации БИОС различных хостов, можно предположить любые объекты, нарушителей и способы реализации в разных комбинациях. Таблица просто для примера.

№	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Специальные службы иностранных государств	Внешний	Система управления и администрирования	Доступ из внешних сетей для (например) блокировки работы инфосистем	Через неправильно настроенное оборудования NAT, firewall к серверам
2	Отдельные физические лица (хакеры)	Внешний	Автоматизированное рабочее место пользователя	Доступ из внешних сетей для создания ботов и т.п.	Через неправильно настроенное оборудования NAT, firewall к АРМ
3	Преступные группы (криминальные структуры)	Внешний	Системы хранения данных (базы данных, СУБД)	Доступ из внешних сетей для кражи информации	Через неправильно настроенное оборудования NAT, firewall к серверам БД
4	Системные администраторы и администраторы безопасности	Внутренний	Все объекты	Доступ через локальную вычислительную сеть организации	Использование учетных записей, обладающих привилегированными правами
5	Авторизованные пользователи систем и сетей	Внутренний	Объекты, доступные после авторизации	Доступ через локальную вычислительную сеть организации	Неправильно настроенные администратором безопасности СЗИ