В своём эссе считаю необходимым рассмотреть проблемы обеспечения безопасности киберфизических систем, используемых в автоматизации кампуса НГУ.

В кампусах НГУ на входе стоят турникеты, которые позволяют пропустить только того, кто сможет пройти процесс идентификации. Для идентификации необходимо предоставить ключ. В основном для прохождения все используют свой пропуск, в котором записан уникальный код, который сравнивается с имеющимися в университетской базе данных. При нахождении совпадения проход разрешается. Каждая попытка прохода регистрируется в базе данных с указанием времени, что позволяет лучше синхронизироваться с камерами видеонаблюдения для распознавания нарушителя.

Для чего НГУ нужно пропускная система? Для чего вообще были установлены турникеты?

Согласно законодательству РФ для противодействия антитеррористической угрозе, каждый ВУЗ должен установить необходимое оборудование, указанное в документе. Например, в приказе **«Об утверждении и введении в действие Руководства по организации и обеспечению комплекса мер по антитеррористической защищенности объектов (территории) ФГАОУ ВО «СПбПУ»»** Указывается понятие *«****Место доступа*** *– место, где непосредственно осуществляется контроль доступа. Например: ворота, калитка, дверь,* ***турникет****, кабина прохода, оборудованные необходимыми средствами защиты.»* Благодаря данному понятию, можно документально регулировать правила прохождения через места доступа, как например: *«Проход через КПП или* ***пункт пропуска****, пост охраны или место доступа со специальными средствами, гражданским, служебным, боевым ручным стрелковым и холодным оружием разрешается:* сотрудникам правоохранительных органов, проводящим оперативно-розыскные мероприятия  *…», а так же «4.2. Постоянная электронная карта (пропуск) является основным документом … для прохода в здания через пост охраны или место доступа и для прохода через входные группы...». Таким образом, данное оборудование не даёт возможность потенциальным нарушителям беспрепятственно входить и выходить (а следовательно, проносить и выносить что – либо) с территории университета, не имея электронный допуск, т.е., не проводя электронную регистрацию прохождения через место доступа.*

Далее попытаемся найти уязвимости в данной пропускной системе и предложить их решения.

Возможность прохождения группой по одному пропуску считаю серьёзным нарушением безопасности, потому что пропускная система должна идентифицировать каждого человека, который пытается попасть или покинуть территория кампуса. Данная уязвимость не позволяет сделать это.

Возможное решение

* Запретить многоразовый вход (выход) через пропускную систему.

Плюсы:

* Невозможно пройти (выйти) группой по одному пропуску.
* Если существует копия пропуска, то возможна ситуация, когда истинный владелец пропуска не сможет пройти. Тогда необходимо будет заменить код в пропуске (при предъявлении соответствующих доказательств) и обновить базу данных, что сделает копию недействительной.

Минусы:

* Увеличение загруженности пропускной системы, т.к. количество непропусков увеличится.
* Увеличение недовольства среди пользователей.

Считаю предложенное решение не самым рациональным, потому что при весомых недостатках не получается полностью решить проблему копий пропусков. Если злоумышленник сделает копию потерянного пропуска и будет избегать ситуаций одновременного использования копии пропуска с оригиналом (например, узнав расписание владельца), владелец никогда не догадается о существовании копии. Такая ситуация ставит под удар легитимного владельца пропуска, потому что копия именно его пропуска была задействована и записана в истории.

Возможное решение:

* Обязать каждого владельца пропуска сообщать об утрате охране, чтобы она удалила из базы данных код утраченного пропуска и выдала новый.

Плюсы:

* Исключает возможность использования скомпрометированного пропуска в любом виде (создание копии или использование чужого пропуска), только если пропуск владелец заранее сообщил о компрометации.
* Всегда будет указан владелец пропуска, по чьей вине произошло нарушение пропускного контроля.

Минусы:

* Главным недостатком считаю то, что при потере пропуска люди, боясь наказания (штраф, выговор и т.д.), начнут искать обходные пути решения вопроса или продолжат пытаться найти свой пропуск (что может продолжаться неопределённое время).

Для этого наказание должно быть максимально допустимо мягким, чтобы человек как можно скорее сообщал охране об утере.

Введение ответственности за несообщение о компрометации пропуска считаю наиболее оптимальным из предложенных вариантов повышения уровня безопасности пропускной системы кампусов НГУ, потому что данное решение не тормозит пропускную систему, не позволяет воспользоваться копией добросовестного владельца, а при наличии сговора всегда будет указано ответственное лицо в истории пропусков.

В заключение своего эссе хотелось бы сообщить, что обеспечение безопасности требует разностороннего рассмотрения каждого вопроса, не только с точки зрения технической реализации, но и с юридической и психологической точки зрения, что значительно усложняет работу эксперта и требует большей квалификации.