

**ФГБОУ ВО БАШКИРСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**



Отчёт по производственной практике

Выполнил студент 2-го курса гр. БИТ 21-16 Галиханов Булат Дамирович

**Институт управления и безопасности
предпринимательства**

**База практики: следственное управление следственного комитета РФ
по РБ Балтачевского межрайонного следственного отдела**



Руководитель от базы практики: Кадыров Аяз Лутфуллович

- центральный аппарат;
- территориальные следственные органы (включая военные);
- образовательные учреждения системы Следственного комитета Российской Федерации;
- научные организации системы;
- организации и подразделения, созданные для выполнения задач, возложенных на СК РФ.

- Под угрозой (вообще) обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Угрозой интересам субъектов информационных отношений будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты АС может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Особые функции, которые должны осуществляться программными средствами, это:

- идентификация объектов и субъектов;
- разграничение (иногда полная изоляция) доступа к вычислительной технике;
- контроль и регистрация действий с информацией и программами.

В процедурах идентификации используются различные методы:

- простые, сложные и одноразовые пароли;
- обмен вопросами и ответами с администратором;
- средства анализа индивидуальных характеристик;
- ключи, магнитные карты, значки и т.д.;
- специальные идентификаторы или контрольные суммы для аппаратуры.

После идентификации защита осуществляется на 3 уровнях:

- аппаратуры;
- программного обеспечения;
- данных.

Основные игроки российского рынка СЗИ от НСД в сегменте Endpoint Security. В настоящее время среди основных игроков рынка СЗИ от НСД в сегменте Endpoint Security можно выделить:

- продукты линейки СЗИ от НСД Secret Net, Secret Net Studio и ПАК «Соболь» («Код Безопасности»);
- продукты линейки СЗИ (СЗИ от НСД, МЭ, СОВ, СКН, СДЗ) Dallas Lock («Конфидент»);
- продукты линейки СЗИ от НСД «Аккорд» (ОКБ САПР);
- СЗИ от НСД «Блокхост-сеть К» и «Блокхост-АМДЗ 2.0» («Газинформсервис»);
- продукты СЗИ от НСД «ПАНЦИРЬ» («НПП «Безопасные информационные технологии»).

Решения для защиты конечных точек (на примере Dallas Lock)

- защита от несанкционированного доступа (НСД) для ОС Windows и Linux;
- персональный межсетевой экран (МЭ);
- система обнаружения и предотвращения вторжений (СОВ);
- средство контроля съемных машинных носителей информации (СКН);
- средство доверенной загрузки (СДЗ) уровня платы расширения;
- система защиты информации виртуальных инфраструктур (СЗИ ВИ) Dallas Lock.

Производственная практика предоставила огромные возможности, такие как:

- изучить дорогое и недоступное ПО, предназначенное для защиты информации;
- отработать навыки, которые в будущем будут необходимы для работы по специальности;
- научиться искать источники угроз, защищаемой информации.

В заключении можно отметить, что все задачи были выполнены, как от руководителя базы практики, так и от руководителя от факультета.

- В целом следует отметить, что на базе практики стоит всё необходимое программное обеспечение, которое позволяет выполнять всю работу. Так как сама организация работает с компаниями поставщиками ПО, то почти все специализированные программы последних версий, со всеми ключевыми "функциями".
- Однако при этом на всех ПК используется ОС Windows 7 и только на некоторых ОС Linux. В качестве рекомендации - обновить Windows 7 до 10 версии, так как в скоро времени прекратится поддержка 7 версии. Ключевым отличием можно выделить следующее: Производительность и безопасность.

Спасибо за внимание!